Preserving the Privacy of a Private Image using Visual Cryptography

M. Baskar[1] T. Gnanasekaran[2] B. Saranya[3]
[1]Associate Professor [2]Professor and Head [3]Software Engineer
[1,2,3]Department of Information Technology
[1,2]R.M.K.College of Engineering and Technology Chennai, India [3]Tech Mahindra Chennai, India

Abstract— Preserving the privacy of pictures keeps exploitation face de identification and face swapping is unreliable since these techniques reduced the chance of automatic face recognition, so the first image is lost. So as to supply additional security to the digital image, visual cryptography is planned. during this case, personal face image is dithered into two host face pictures that square measure keep in two different online servers specified the private image is discovered only each sheets square measure at the same time accessible. At a similar time, the individual sheet pictures don't reveal the identity of the non-public image.

- The possibility of hiding a private face image in two host face images and successful matching of face images reconstructed from the sheets.
- The inability of sheets to reveal the identity of the private face image.

Key words: Face Swapping, Face De-Identification, Face, Privacy, Visual Cryptography

I. INTRODUCTION

Bio-Metric has been accustomed establish a human supported the various pattern owned by the human. The individuality of the pattern is one advantage of biometric, since the pattern is almost not possible to be imitated by others. The most concern in biometric is finding a pattern to unambiguously establish people. Another concern is that the pattern should not be simply modified by natural causes, e.g. temperature, climate, age, illness, etc. Some biometric patterns that are used are finger print, palm print, and iris. The term "privacy" as employed in this paper refers to the de-identification of face pictures. To preserve the privacy to face pictures gift in police investigation videos, Newton et al. [1] and Gross et al. [2] introduced a face de-identification algorithmicrule that reduced thepossibilities of playing automaticfacerecognition whereas protective detail softheaded like expression, gender, and age. Betook et al. [3] projected a face swapping technique that protected the identity of a face image by mechanically subbing it with replacements taken from an outsized library of public face pictures. However, within the case of face swapping and aggressive de-identification, the first face image will be lost. during this paper, the employment of visual cryptography is explored to preserve the privacy of raw pictures by rotten the first image into two pictures in such the way that the first image will be disclosed only each pictures are at the same time available; additional, the individual host pictures don't reveal any info concerning the first image. Throughout the enrollment method, the non-public face image is shipped to a trustworthy third-party entity. Once the trustworthy entity receives it, knowledge is rotten into two pictures and therefore the original data is discarded. The rotten elements are then transmitted and keeping two totally different on-line servers such the identity of the non-public information isn't disclosed to either server. Throughout the authentication method, the trustworthy entity sends a call for participation to every server and therefore the corresponding sheets are transmitted thereto. Sheets are overlaid (i.e., superimposed) so as to reconstruct the non-public Once the matching score is computed, there constructed image is discarded.

For finger prints, 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. 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.

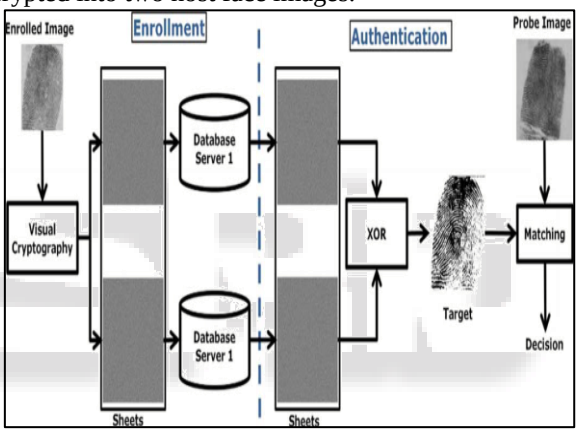

Fig. 1: Proposed Approach for De-Identifying and Storing a Finger Print Image.

A similar technique is used for iris codes.

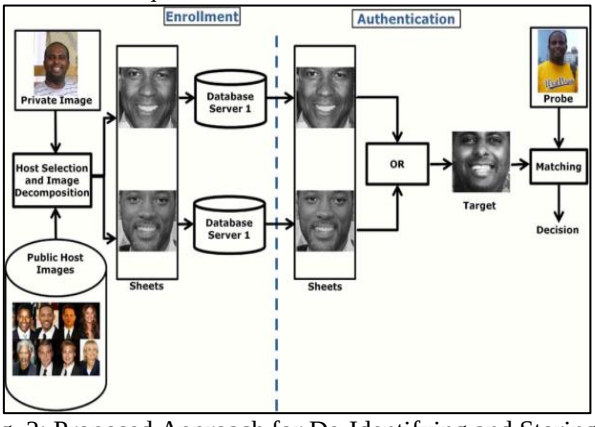

Fig. 2: Proposed Approach for De-Identifying and Storing a Face Image.

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.

- 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.

- A set of public face images may be used to host the private face image. In essence, a small set of public images can be used to encrypt the entire set of private face images.
- Using no face 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

A. Diversity:

For finger prints, the sheets appear as random noise making it difficult to match them.

B. Revocability:

To strengthen security, the decomposing operation can be periodically invoked at regular time intervals.

C. Security:

There have been numerous efforts in the literature to guarantee that the data passed across network are protected from unauthorized modification and inaccurate updates.

D. Performance:

The recognition performance due to the reconstructed image is not degraded after decryption.

II. VISUAL CRYPTOGRAPHY

One of the best known techniques to protect data such as biometric templates [4] 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 [5] 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. 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. In the case of (2, 2) VCS, each pixel in the original image is encrypted into two sub pixels 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 share 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 can be determined. If 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 [6]. However, the original image will become visible.

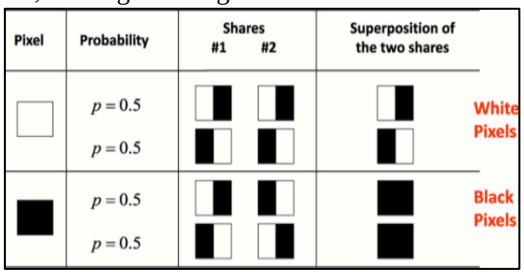

Fig. 3: Illustration of a 2-Out-Of-2 VCS Scheme with 2 Subpixel Constructions

In 2002, Nakajima and Yamaguchi [7] 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.

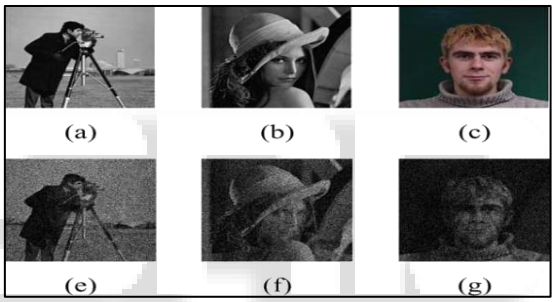

Fig. 4: Encryption of a Private Face Image in Two Standard Host Images. (a)Host 1: Cameraman Image. (B) Host 2: Lena Image. (C) A Private Faceimage. (E) And (F) The Two Host Images After Visual Encryption (Two Sheets).(G) Result Of Superimposing (E) And (F).

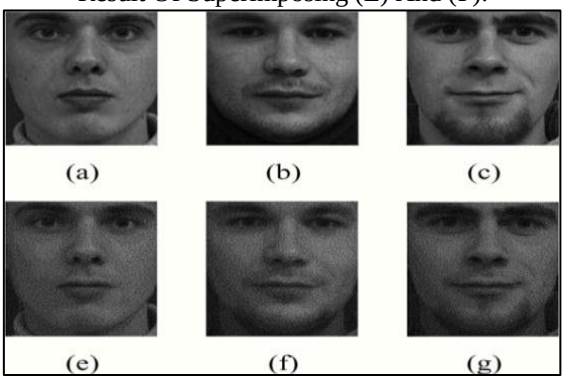

Fig. 5: Encryption of A Private Face Image In Two Prealigned And Cropped Faceimages. (A) And (B) Are Two Host Images. (C) Is A Private Face Image. (E) And (F) Are The Host Images After Visual Encryption (Two Sheets). (G) Is The Result Ofoverlaying (E) And (F).

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:
The original image that has to be hidden. In our application, this is the private face image.
2) Hosts:
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:
The secret image is encrypted into sheet images which appear as random noise images (in the case of VCS) or as a natural host image (in the case of GEVCS).
4) Target:
The image reconstructed by superimposing the sheets.
5) Sub pixel:
Each pixel is divided into a certain number of sub pixels during the encryption process.
6) Pixel Expansion:
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 collections of black-and-white sub pixels.
These collections of sub pixels are known as shares.
8) Relative Contrast:
The difference in intensity measure between a black pixel and a white pixel in the target image.
9) OR-ed-vector:
A matrix is transformed to an –dimensional vector by applying the Boolean OR operation across each of the columns.
10) Hamming weight:
The number of "1" bits in a binary vector

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

The 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. This is explained in more detail below.
1) Digital Half Toning and Pixel Expansion:
Digital half toning is a technique for transforming a digital gray-scale image to an array of binary values represented as dots in the printing process [8]. Error diffusion is a type of half toning technique in which the quantization error of a pixel is distributed to neighboring pixels which have not yet been processed. Floyd and Steinberg [9] 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 equaling the number of sub pixels per share, .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. In our application, the host images used for encrypting a private face image and the private image itself are converted to half toned images.
2) Encryption:
The encryption process is applied on a pixel-by-pixel basis using the three half toned 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 security of the scheme is also important. Therefore, during encryption, a Boolean matrix is randomly selected from a set of Boolean matrices for every pixel in the original image.

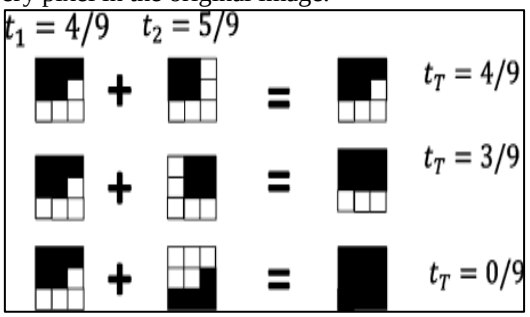

Fig. 6: Examples of Subpixel Arrangements.

III. SECURING FINGERPRINT TEMPLATES

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 [10]. Furthermore, the target image can be down-sampled by reconstructed image will be visually appealing while requiring less storage space.

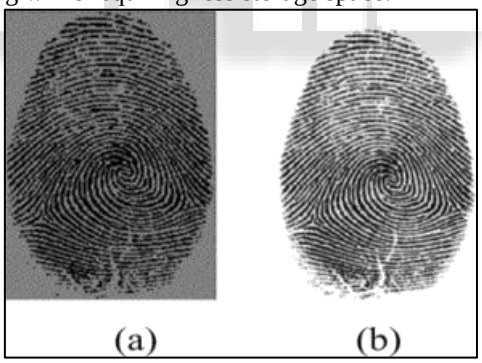

Fig. 7: Reconstructed Fingerprint Image When Using The (A) OR And (B) XOR Operators.

Fig. 7shows 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

The first task is to select two host images. 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 may become perceptible. This issue can be mitigated if the host images for a particular private image are carefully chosen.

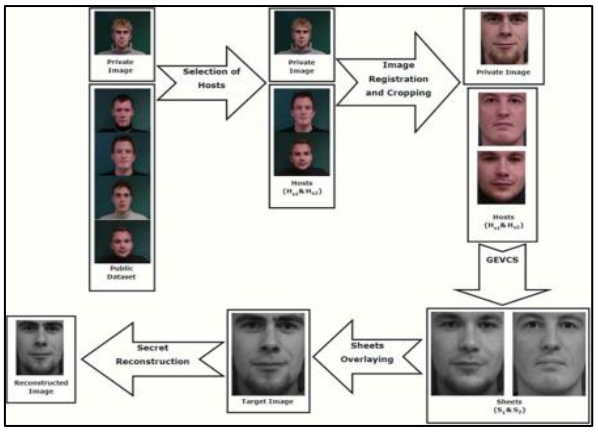

Fig. 8: Block Diagram of the Proposed Approach for Storing and Matching Face Images

Fig.8 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. An active appearance model (AAM) [11] that characterizes the shape and texture of the face is utilized to determine the similarity between the private face image and host images (Fig. 8)

1) Building the AAM:

Four steps are needed for building a basic AAM from a set of training images.

1) 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.
2) Building the Shape Model: A shape alignment process is performed to remove the effects of affine transformations (translation, scaling, and rotation).
3) 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 are consolidated to create a texture model.
4) Building the Combined AAM: Shape and texture are often correlated and, so, PCA is once again used to construct a compact model from shape and texture model. This helps in synthesizing an image with a given shape and texture.

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 and the synthesized image needs to be minimized.

B. Selection of Hosts:

For selecting compatible hosts, the cost of registering each image in the public dataset with the private image is computed. These costs are sorted in order to locate two host images, and which have the smallest registration cost.

1) Transformation Cost:

This cost measures the amount of geometric transformation necessary to align two images based on the annotated landmarks generated by the AAM. The transformation cost is the measure of how much transformation is needed to align the two face images by utilizing the thin model, which is the bending energy necessary to perform the transformation.

2) Appearance Cost:

First, the private face image and the host image are normalized by warping them to the mean shape, resulting in shape-free texture images and host images. This normalization step uses the mean shape computed during the AAM training phase.

C. Image Registration and Cropping:

In this step, the global affine transformation component of the thin model is used to align the two selected host images with the secret image . Next, the aligned hosts and the secret image are cropped to capture only the facial features which have been located by AAM.

D. Secret Encryption and Reconstruction:

GEVCS is used to hide the secret image in the two host images resulting in two sheets.S1 and S2 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

In the experiments, the impact of varying the number of images in the public dataset was investigated.

1) Experiment 1: 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. 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. The images are reconstructed when host images are selected using (a) the transformation cost only and (b) the sum of the normalized transformation cost and appearance cost.
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, two fixed face images as hosts, was used. For each subject in the private dataset, one frontal face image was selected as the secret image to be encrypted by the two host face images. The reconstructed images were observed to match very well with the original images.

4) Experiment 4: 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 same subject were first computed. Next, the reconstructed images and the corresponding sheets were independently used in the matching process.

5) Experiment 5: In this experiment, the hided layer contained host images are send through network. For whom to get proper key information they only decrypt the host image into hided secret image; This type of hiding image of two independent public face images such that the original face image can be reconstructed only when both the public images are available. When the private face image has to be matched, 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.

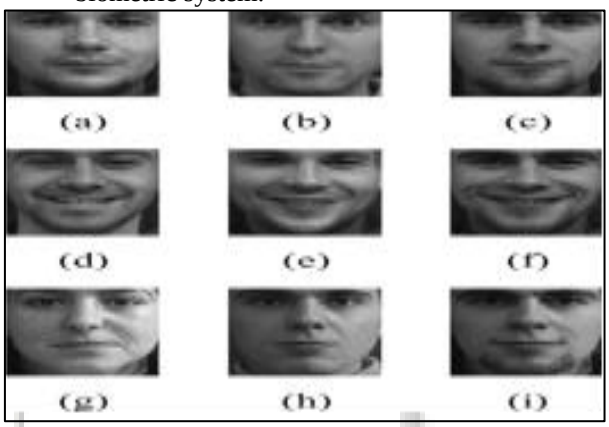

Fig. 9: Examples from Experiment 4 Where (A), (D), and (G) Are The First Sheets And (B), (E), And (H) Are The Second Sheets. (C), (F), And (I) Are The Corresponding Reconstructed Face Images.

Fig. 9 shows that each subject in the private dataset has three reconstructed images.

VI. Conclusion and Discussion

This work explores the chance of using visual cryptography and life science for transmission privacy. during this paper a way is planned to enhance the authentication of image, visual cryptography and biometric template are used, to confirm that the one that is accessing the image is a certified one. If he is a certified person then the system revels the first image. The system is additional difficult, however provides additional security and authentication. And victimization alternative sort of visual cryptography significant share is generated that can also be applied. The biometric templates are susceptible to stealing thus additional secured templates are required for secret writing and cryptography. The contribution of this paper includes a strategy to shield the privacy of a face image by moldering it into 2 freelance sheet pictures specified the personal face image are often reconstructed only if each sheets are at the same time out there. The proposed algorithmic program selects the host pictures that are presumably to be compatible with the key image based on pure mathematics and look. GEVCS is then wont to write the personal image within the elite host pictures. it's determined that the reconstructed pictures ar kind of like the first personal image. Increasing the peel growth issue will cause a rise within the storage requirements for the sheets. Within the recent literature there are some efforts to develop a VCS while not pel growth [12], [13]. However no such theme presently exists for generating sheets that don't seem to be random clattery pictures. Thus, more work is important to handle this drawback.

References

[1] 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.
[2] 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.
[3] D. Bitouk, N. Kumar, S. Dhillon, P. Belhumeur, and S. K. Nayar, "Faceswapping: Automatically replacing faces in photographs," ACMTrans. Graph., vol. 27, no. 3, pp. 1–8, 2008.
[4] B. Moskovich and M. Osadchy, "Illumination invariant representationfor privacy preserving face identification," in Proc. IEEE Computer Society and IEEE Biometrics Council Workshop on Biometrics, San Francisco, CA, Jun. 2010, pp. 154–161.
[5] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, and B. Kumar, "Biometric encryption," in ICSA Guide to Cryptography. New York: Mc-Graw-Hill, 1999.
[6] M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT,1994, pp. 1–12.
[7] M. Nakajima and Y. Yamaguchi, "Extended visual cryptography for natural images," J. WSCG, vol. 10, no. 2, pp. 303–310, 2002.
[8] S. Shevell, The Science of Color. Amsterdam, The Netherlands: ElsevierScience Ltd., 2003.
[9] R. Floyd and L. Steinberg, "An adaptive algorithm for spatial greyscale," SPIE Milestone Series, vol. 154, pp. 281–283, 1999.
[10] 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
[11] T. Cootes et al., "Active appearance models," IEEE Trans. Pattern Anal. Mach. Intell., vol. 23, no. 6, pp. 681–685, Jun. 2001.
[12] 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.
[13] 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

