A VISUAL CONFIDENTIAL SHARING SCHEME FOR MULTIPLE PROFICIENT SYSTEMS BY CRYPTOGRAPY WITHOUT PIXEL EXTENSION

B.Sudhanthira Priya[1] V.Sundhara raj[2]

[1]PG Scholar, Department of Electronics and Communication Engineering,
Paavai College Of Engineering, Nammakal, India.

[2]Assistant Professor, Department of Electronics and Communication Engineering,
Paavai College Of Engineering, Nammakal, India.

E-mail:-freedompriyaeie@gmail.com

***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. In this paper, we propose a novel VCS scheme that can share two binary secret images on two rectangular share images with no pixel expansion. The experimental results show that the proposed approach not only has no pixel expansion, but also has an excellent recovery quality for the secret images. As our best knowledge, this approach that can share multiple visual secret images without pixel expansion.**

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

I. INTRODUCTION

BIOMETRICS is the science of establishing the identity of an individual based on physical or behavioural traits such as face, fingerprints, iris, gait, and voice .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 privacy1 to the subject by adequately protecting the contents of the database. For protecting the privacy of an individual enrolled in a biometric database, storing a transformed biometric template instead of the original biometric template in the database. This was referred to as a private template or a cancelable biometric. And a three-step hybrid approach that combined the advantages of cryptosystems and cancelable biometrics. Apart from these methods, various image hiding approaches have been suggested by researchers to provide anonymity to the stored biometric data. For according privacy to face images present in surveillance videos, 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. 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, a method to perform secure face identification by representing a private face image with indexed facial components extracted from a public face database.

The use of visual cryptography is explored to preserve the privacy of biometric data 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. 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, steganography, or cryptosystem 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, 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, each private face image is decomposed into two independent public host images.

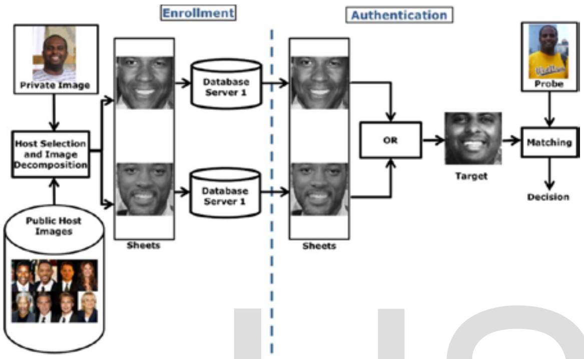

Fig. 1. Approach for de-identifying and storing a face image.

In this scenario, the private image can be viewed as being encrypted into two host face images. The use of face images as hosts for a private face image 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 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. 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.

II. VISUAL CRYPTOGRAPHY

One of the best known techniques to protect data such as biometric templates 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 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. In the case of (2, 2) VCS, each pixel 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 can be determined. If 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 there will be a 50% loss in contrast. However, the original image will become visible.

III. SECURING IRIS AND FINGERPRINT TEMPLATES

The use of basic visual cryptography for securing fingerprint and iris templates was suggested in reference; 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, 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. Furthermore, the target image can be down-sampled by reconstructing just one pixel from every block. Thus, the reconstructed image will be visually appealing while requiring less storage space. 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.

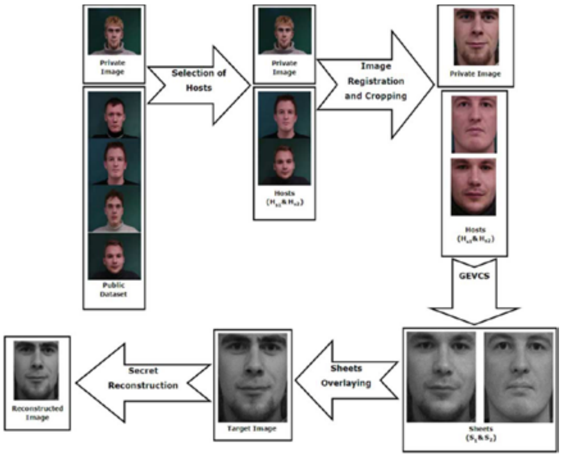

Fig. 2. Block diagram of the for storing and matching face images.

IV. PROPOSED VISUAL SECRET SHARING SCHEME WITHOUT PIXEL EXPANSION

In this section, the details are described of our visual multiple secrets sharing scheme, with no pixel expansion and which does not need a pattern book. The no pixel expansion and no patterns book characteristics of our proposed scheme can be best understood
by the following description, and the contrast factor is explained by the next section of experiments. The proposed scheme adopted two rectangular share images to share two rectangular secret images. The rotation degree was 180_ for revealing the second secret image. As with the previous schemes, encrypting and decrypting processes were needed. In our proposed scheme, encryption included 3 processes:

A. DSP (dividing and separating process).

B. SP (sticking process).

C. CMP (camouflaging with maximum block density process).

A. DSP: dividing and separating process

At the beginning, two empty share images (i.e., the pixel color is white) with a size equal to that of the secret image must be generated. Then, each secret image must be divided into K blocks with n _ n size, that is K = (h/n) _ (w/n). According to the position of each black pixel and the sum of black pixels on the block, one block can be randomly separated to two subsets without any one black pixel being overlapped, and the difference in the number of black pixels between the two subsets must be equal to or less than one. For one block, the two subsets are noted as Cqand Cq+1,

B. SP: sticking process

The sticking operation executes a logic ‘‘OR” operation between the separated subset and the share images during the sticking process. The goal is to build the patterns of two blocks b1,k and b2,k for share images S1 and S2. The sticking results are generated according to the decrypting function. By the defined decrypting process in our proposed scheme, secret image SE1 is revealed by directly stacking share images S1 and S2. But, it needs to rotate the share image S2 with 180_ angle and stack with S1.

C. CMP: camouflaging with maximum block density process

In order to make the share image meaningless to anyone but an unauthorized user, two camouflaging processes must be executed for every block of two share images obtained from the sticking process. Based on the maximum of block density, the camouflaging process makes the black pixel density of every block equal, so that every block appears to have the same pattern and the whole image will be a meaningless image.

V. EXPERIMENTS AND RESULTS

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

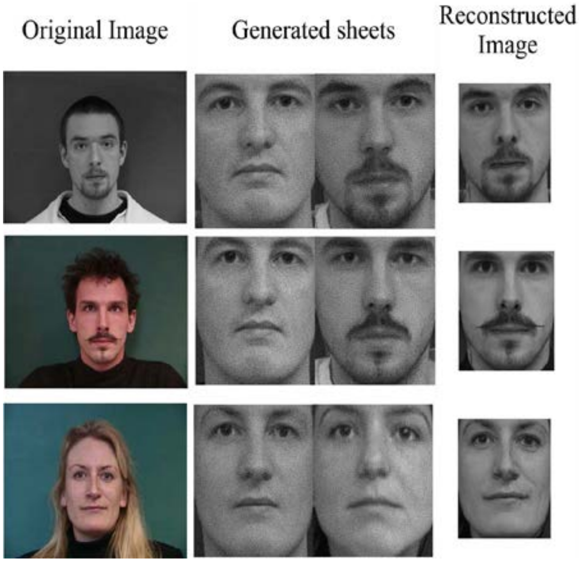

Fig. 3. Illustration of the proposed approach using images from the IMM database.

VI CONCLUSION

In this paper, a visual multiple secrets sharing scheme with no pixel expansion has been proposed. To the best of our knowledge, this is the first paper for sharing two secrets with no pixel expansion and not using a codebook to encrypt the secret images. Under the aspect ratio constraint, the least pixel expansion was 4 times that of previous schemes for sharing two secrets. Compared to other schemes, it was clear that the pixel expansion problem in VSSM could be solved by our proposed scheme. Through the separation and camouflaging processes, two share images became meaningless images which did not leak any information of the secret images, and so conformed to the security rule of visual secret sharing schemes. To reveal the secret image, the two share images were just stacked and the recovery image could be recognized by the human visual system. No other devices were needed to reveal the secret image. Our proposed scheme achieved the purpose of a visual secret scheme by not only solving the critical problem of pixel expansion, but it also adopted a novel study completely different from that of previous schemes. Further research for this proposed scheme will study the sharing of more than two secrets and propose another camouflaging process.

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.
[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,” ACMTrans. 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: Mc- Graw-Hill, 1999.
[17] M. Naor and A. Shamir, “Visual cryptography,” in Proc. EUROCRYPT, 1994, pp. 1–12.