Annals of DAAAM for 2012 & Proceedings of the 23rd International DAAAM Symposium, Volume 23, No.1, ISSN 2304-1382
ISBN 978-3-901509-91-9, CDROM version, Ed. B. Katalinic, Published by DAAAM International, Vienna, Austria, EU, 2012
Make Harmony between Technology and Nature, and Your Mind will Fly Free as a Bird
Annals & Proceedings of DAAAM International 2012

A NEW FRAMEWORK FOR BIOMETRIC FACE RECOGNITION USING VISUAL CRYPTOGRAPY

MIHAILESCU, M[arius] I[ulian] & PIRLOAGA, M[arian] D[orin]

Abstract: The paper presents a new framework for biometric face recognition based on visual cryptography techniques. The framework is developed using .NET technologies (C# 4.0) and the implemented algorithm in C# will consist in three stages which are described later in detail. The role of visual cryptography will be to protect the image and, with the help of RSA, it will create a secret visual cryptography scheme which will protect the image from malicious persons.
Keywords: *biometrics, face recognition, visual cryptography, RSA, VSS*

1. INTRODUCTION

Visual cryptography [1] represents a cryptographic method which gives us the possibility for visual information (pictures, text etc.) to be encrypted in a way that the decryption can be done by the human visual system without the help of computers.

The paper's idea is to build a cryptosystem that will help security biometric systems that regard face recognition characteristics.

The algorithm used for encryption generates a cipher image that is sent to the receiver through a communication channel. When the cipher is received at the destination, the system or user sets the key and the original image will be decrypted. In the Figure 1 we can see the block diagram of the cryptographic system. The dimension of the key is between 50 and 256 bits with the possibility to extend her length to 512 bits. We have taken into consideration two important characteristics to determine the efficiency of the proposed cryptographic systems [2]:

a. Quality of the image that is being reconstructed, and
b. The resizing of factor value.

If exists any kind or type of loss information in process of reconstruction phase, this will lead to the reduction of the quality of the recovered image.
In most cases an image is represented as RGB color space [3, 4], because the computers, as input and output devices, use this color system. Each vector is formed of three components that represent the intensity values in red, green, and blue channel. If a change is made in the intensity value this changes the information stored in the picture. In this case, by performing some changes in intensity values, the encryption process of the image can be done and the reverse process of decryption will be successfully completed. In the case of changes that take place separately on red, green and blue layers, we will have a more robust visual cryptographic system. That is due to the fact that, if an intruder goes for complete analysis of the image, he will try to find out these basic intensity values. These intensity values will help the intruder to generate the original image. In this case, if the encryption was done at this low level (basic level), will be very difficult to break the system.

All the changes regarding the intensity values are made using mathematical functions.

This paper is organized as follows:

Section 2 represents a state of the art of the most important aspects and schemes regarding visual cryptographic, starting with the most important one [1]. *Section 3* represents the entering point for the proposed idea; the framework and the architecture of the solution are presented in detail. *Section 4* represents the visual cryptographic scheme and the integration and how the implementation of RSA algorithm is done for face recognition. There is also a small mathematical background for the primary functions. In this section there is also the algorithm for encryption and decryption presented. In *Conclusions* section there are presented also some experimental results.

The application (framework) is developed using C# 4.0 as programming language. For those who are interested in seeing how the application is running and to study the source code, please send an e-mail to mihmariusiulian@gmail.com. For source code you need to install Microsoft Visual Studio Express 2010 with C# or Microsoft Visual Studio 2010 Ultimate.

2. STATE OF THE ART

This section will go through the most important visual cryptographic schemes. The concept of visual cryptography was first introduced in 1994 by Naor and Shamir [1]. In [1], the proposed encoding scheme divides the binary image into two shares, *FirstShare* and *SecondShare*. If one pixel is white then the one row of the above is chosen to generate *FirstShare* and *SecondShare*. It's the same thing if the pixel is black. Each share *p* pixel is encoded into two white and two black pixels. Each share alone gives no possibility to figure out if the pixel *p* is white or black.In [2], the authors propose a technique to hide a binary image into two meaningful shares by using spatial domain image hiding schemes. Note that the two secret shares are

embedded into two gray-level cover images, and that, to decode the hidden messages, embedding images can be superimposed. Ligu Fang [3] proposes a (2,n) scheme based on combination. For error correcting code was suggested by [6] a threshold visual secret sharing schemes that represent a mixed between XOR and OR operation with reversing.

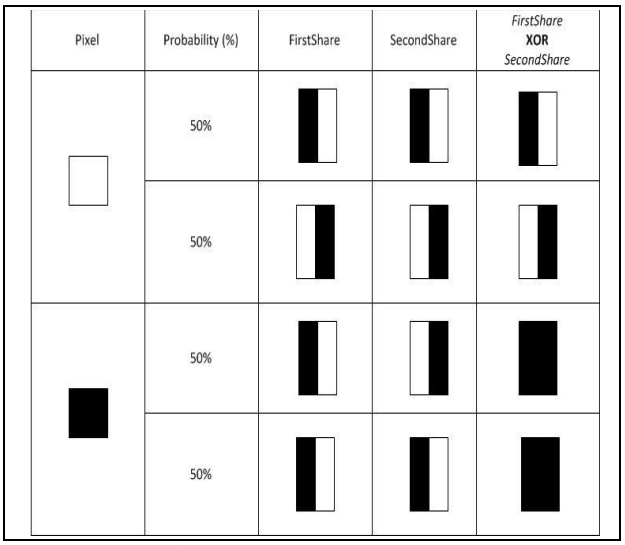

Fig. 1. The scheme for encoding a binary pixel into two shares, proposed by Naor and Shamir [1]

3. PRESENTATION OF THE IDEA. FRAMEWORK INTRODUCTION

Newton et al. [4] and Gross et al.[5] propose a face de-identification algorithm which focuses on the minimized probability of the automatic face recognition proces, having in consideration the preserving of details of the face, such as expression, gender and age.

The proposed method takes into considerations also the template protection requirements:

- **Diversity and Revocability Metrics.** Various types of application will engage different public datasets used for image selection. The hosts selected to encrypt a private face image can be different across various applications. It is absolutely necessary to revoke the stored templates and reissue new templates for a new face image by changing hosts [23-38].
- **Security and Performance Metrics.** It is very hard to computationally obtain the original face image. The obtaining process is accomplished from individual stored templates by means of visual cryptography [10-25, 39-41].

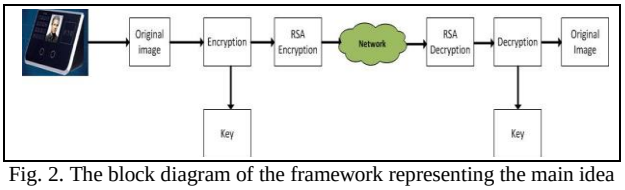

Fig. 2. The block diagram of the framework representing the main idea

In Figure 2, the process is illustrated very clearly. In the first phase the person will stand in front of a device and his image will be scanned. The original image will be encrypted with a key. The encryption will be symmetric. After the image is encrypted with symmetric algorithm, the RSA encryption is done on that package. In this case we have two encryption steps. First step is a classic algorithm such as AES, *TripleDES* or DES with the length of the key of between 50-256 bits. The *second step* is formed from a public key algorithm RSA. This will lead to a stronger encryption of the image [4].
The framework generates another image that will be similar to a layer over the image captured from the device. After the encryption is done, with the two steps mentioned above, the encrypted package will be stored in another image.The visual cryptographic scheme will be stored in the template and the decryption process will be made at the database level by the algorithm discussed in Section 4.The main scheme is referred to as the *k*-out-of-*n* visual cryptography scheme. The VSS is denoted as *(k,n) VCS.* In our case the original binary image will be encrypted in *n* images, such as:

$$T = S_{h_1} \oplus S_{h_2} \oplus S_{h_3} \oplus \ldots \oplus S_{h_k} , \qquad (1)$$

Where $\oplus$ represents a Boolean operationS_{h_1}., $h_i \in 1,2,\ldots,k$ representing the image that will appear as a white noise, $k \leq n$, and n represents the number of noisy images. It is extremely difficult to decrypt the image T using an individual $S_{h_i}{}'s$.Starting from the definitions established below, the scheme model is defined:

- *The Human Image (HI).* Represents the image captured from the readerai device (see Figure 1 – first component from the left).
- *The Random Image (RI).* Represents an image which is generated automatically by the system. This image, seen as a layer, will be overlapped over the original.
- *The Secret Image (SI).* Represents the image in which the original will be hided.
- *The host.* Represents the images that will be used to encrypt the secret image by using a gray level, usually known as Gray-level Extended Visual Cryptography Scheme. In our framework this is represented as corresponding to the face images that are in the public data set.
- *Templates.* The image will be encrypted into different *n* small templates that will compound a standard template. This will appear as randomly noise in images (here it is about *(k,n)* visual cryptographic scheme) or as a normal picture (here it is about the case of GEVCS).
- *Target (TA).* Represents the image that is rebuilded by stacking or by superposition the small templates.
- *The expansion of the pixels (EP).* Represents the number of sub-pixels used by the small templates represented by small images used to encode each pixel from the original image.
- *The shares (SH).* Represents the encryption of each pixel that will be encrypted using a set of *n* collections of *m* black and white sub-pixels.
- *Relative contrast (RC).* Represents the difference in intensity that is measured between two different pixels, one black and another one white in the destination image.
- *The Hamming weight (HAM(V)).* Represents the '1' bits from the binary vector.

All this aspects discussed above represent the kernel of the application and they are integrated into the framework.

In Figure 3 we can see a detailed overview of the framework and how it is working in real life.

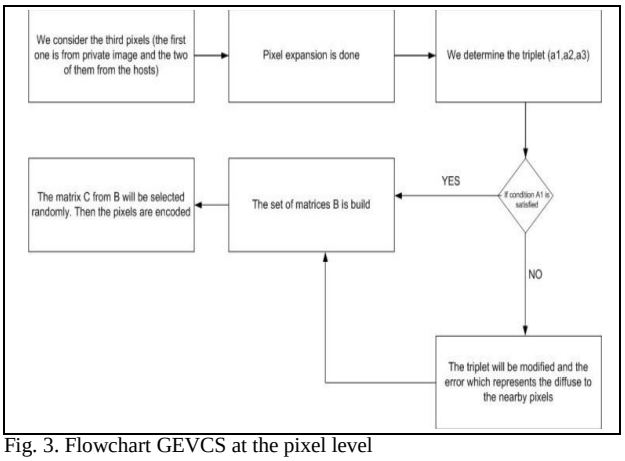

Fig. 3. Flowchart GEVCS at the pixel level

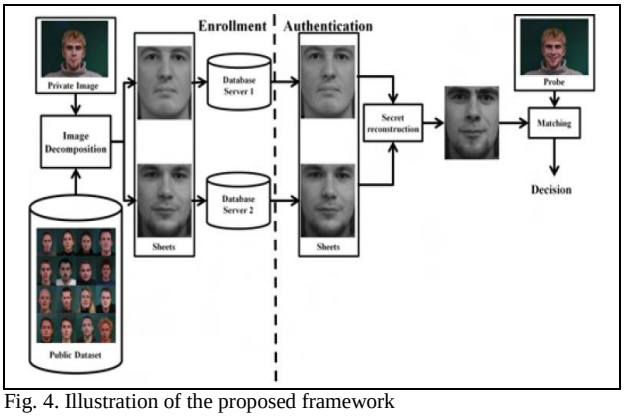

Fig. 4. Illustration of the proposed framework

4. VISUAL CRYPTOGRAPHY SCHEME AND IMPLEMENTATION. MATHEMATICAL BACKGROUND

The function used in the application has a bijective mapping i.e. function has one-one and onto mapping. This demonstrates the inverse of the existing function. In this case, the original information of the image will be retrieved back during the decryption process without facing any error [46-49]. The function is:

$$(2) \qquad g(a) = abs\left(\frac{1}{\log\left(\tan\left((\exp(x)*\cos(\exp(1))*\sin(\exp(A)))\right)\right)}\right),$$

where *x* and *'1'* represent the key and *'A'* represents the *gcd* of the two keys used in the encryption process.

3.1. The Encryption Process

Step 1: The image of the human is read, the keys k1 and k2 are generated and the factor value will be generated the same;
Step 2: The function g() is generated and will contain some values generated from a function found in an array;
Step 3: There is an absolute value needing to be found for function g().
Step 4: The A will be calculated as A = gcd (k1, k2);
Step 5: The next step will consist in passing the values to the low pass filter;
Step 6: The image will be resized using a type of interpolation named bi-cubic and the RGB layer will be obtained in a separate matrix with the factor which was generated in the first step;
Step 7: The pixel values will be multiplied with the absolute value calculated above;
Step 8: The Red matrix which is upside-down is flipped;
Step 9: The Green matrix which is left-side right is flipped;
Step 10: The Blue matrix is rotated with factor value;
Step 11: The RSA is applied on the encrypted structure;
Step 12: The image will be generated again and it will saved as a specific format;
Step 13: The encryption package is send over the network;

3.2 The Decryption Process

As we know, the decryption is the reverse process of the encryption process. The decryption algorithm consists in *n* steps.

Step 1: The image is received and the key and the factor for resizing are needed to be provided;
Step 2: The image is split into red, green and blue parts;
Step 3: The red matrix which is upside down will be flipped;
Step 4: The green matrix which is left-side right is flipped;
Step 5: The blue matrix will be rotated twice using the factor value;
Step 6: The function will be generated using the keys.
Step 7: The A will be calculated as A = gcd (k_1, k_2);
Step 8: The absolute value of the function needs to be found and pass it to the low pass filter;
Step 9: The received image will have the pixel values divided using the absolute value of the function;
Step 10: The RSA decryption process is applied;
Step 11: The image will be formed;
Step 12: The image will be resized by multiplying the rows and columns with the bi-cubic interpolation.

5. CONCLUSION

The paper presents a new framework of visual cryptographic system which can successfully be used in face recognition biometric systems. The main idea behind this framework is that it can be used to hide the original image information from a malicious person or unauthenticated user. The advantages of the proposed method consist in the resizing factor and in the possibility to reconstruct the secret image. Another important aspect is confidentiality and the authentication that can be verified by digital signatures. The proposed method can be a good suggestion for secure visual data transmission in a system that has limited bandwidth. The idea can be applied in government agencies, secret services, military services field, university research departments etc.

6. REFERENCES

[1] M. Naor and A. Shamir, "Visual Cryptography", Advances in Cryptology – EUROCRYPT, pp 1-12, 1994

[2] C. C. Chang, J. C. Chuang, and P.Y. Lin, “Sharing A Secret Two-Tone Image In Two Gray-Level Images”, Proceedings of the 11th International Conference on Parallel and Distributed Systems (ICPADS’05), 2005

[3] L. Fang and B. Yu, “Research On Pixel Expansion of (2,n) Visual Threshold Scheme”, 1st International Symposium on Pervasive Computing and Applications, pp. 856-860, IEEE

[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”, IEEE Workshop on Privacy Research in Vision, 2006

[6] X. Q. Tan, “Two Kinds of Ideal Contrast Visual Cryptography Schemes”, International Conference on Signal Processing Systems, pp. 450-453, 2009

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

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

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

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

[11] 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

[12] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, and B. Kumar, “Biometric encryption,” ICSA Guide to Cryptography , 1999

[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. 67–585, 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

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

[24] 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

[25] 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

[26] U. of Stirling. Psychological image collection at stirling (pics). http://pics.psych.stir.ac.uk/

[27] E. Osuna, R. Freund, and F. Girosi. Training support vector machines: An application to face detection. Proceedings of the IEEE Conf. Computer Vision and Pattern Recognition, pages 130–136, June 1997

[28] K. Pearson. On lines and planes of closest fit to systems of points in space. Philosophical Magazine, 2(6):559–572, 1901

[29] P. Phillips, H. Moon, S. Rizvi, and P. Rauss. The feret evaluation methodology for face-recognition algorithms. IEEE Transactions on Pattern Analysis and Machine Intelligence, 22(10):1090–1104, October 2000

[30] S. Pigeon and L. Vandendrope. The m2vts multimodal face database. In Proceedings First International Conferenbce on Audio- and Video-Based Biometric Person Authentication, 1997

[31] F. Raphael, B. Olivier, and C. Daniel. A constrained generative model applied to face detection. Neural Processing Letters, 5(2):11–19, April 1997

[32] S. A. Rizvi, P. J. Phillips, and H. Moon. The feret verification testing protocol for face recognition algorithms, 1999

[33] H. A. Rowley, S. Baluja, and T. Kanade. Neural network-based face detection. IEEE trans. Pattern Analysis and Machine Intelligence, 20(1):23–38, January 1998

[34] F. Samaria. Face Recognition Using Hidden Markov Models. PhD thesis, University of Cambridge, 1997

[35] F. Samaria and A. Harter. Parameterisation of a stochastic model for human face identification. In Proceedings of 2nd IEEE Workshop on Applications of Computer Vision, Sarasota, FL, USA, December 1994. DB abailable at http://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html

[36] H. Schneiderman and T. Kenade. Probabilistic modeling of local appearance and spatial relationships for object recognition. Proc. IEEE Conf. Computer Vision and Pattern Recognition, pages 45–51, 1998

[37] S. Srisuk and W. Kurutach. Face recognition using a new texture Representation of face images. In Proceedings of Electrical Engineering Conference, pages 1097–1102, Cha-am, Thailand, November 2003

[38] S. Srisuk, M. Petrou, W. Kurutach, and A. Kadyrov. Face authentication using the trace transform. In Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, CVPR’03, pages 305–312, Madison, Wisconsin, USA, June 2003

[39] T. J. Stonham. Practical face recognition and verification with wisard. In H. D. Ellis, editor, Aspects of face processing. Kluwer Academic Publishers, 1986

[40] K.-K. Sung. Learning and Example Selection for Object and Pattern Detection. PhD thesis, Massachusetts Institute of Technology, 1996

[41] L. Torres. Is there any hope for face recognition? In Proc. of the 5th International Workshop on Image Analysis for Multimedia Interactive Services, WIAMIS, Lisboa, Portugal, 21-23 April 2004

[42] Arathi Arakala, Jason Jeffers and Kathy J. Horadam. Fuzzy Extractors for Minutiae-Based Fingerprint Authentication. In International Conference on Biometrics, 2007

[43] Ileana Buhan, Jeroen Doumen, Pieter Hartel and Raymond Veldhuis. Feeling is Believing: a secure template exchange protocol. In International Conference on Biometrics, volume 4642 of LNCS, pages 897-906, 2007

[44] Ileana Buhan, Jeroen Doumen, Pieter Hartel and Raymond Veldhuis. Constructing practical fuzzy extractors using QIM. Centre for Telematics and Information Technology, University of Twente, Netherland Technical Report TR-CTIT-07-52. 2007

[45] E.J.C Kelkboom, B. G\"okberk, T.A.M. Kevenaar, A.H.M. Akkermans and M. van der Veen. "3D Face": Biometric Template Protection for 3D Face Recognition. In International Conference on Biometrics, volume 4642 of LNCS, pages 566-573, 2007

[46] Karthik Nandakumar, Anil K. Jain and Sharath C. Pankanti. Fingerprint-Based Fuzzy Vault: Implementation and Performance. IEEE Transactions on Information Forensics and Security, 2(4):744-757, 2007

[47] Walter J. Scheirer and Terrance E. Boult. Cracking Fuzzy Vaults and Biometric Encryption. In Biometrics Symposium, 2007

[48] E. Maiorana, P. Campisi and A. Neri. Biometric Signature Authentication Using Radon Transform-Based Watermarking Techniques. In Biometric Symposium, 2007

[49] A. Goh and D.C.L. Ngo. Computation of cryptographic keys from face biometrics. In International Federation for Information Processing, volume 2828 of LNCS, 2003