Application of visual cryptography for learning in optics and photonics

Avikarsha Mandal*[a], Peter Wozniak[a], Oliver Vauderwange[a], Dan Curticapean[a]
[a] Offenburg University, Badstr. 24, 77652 Offenburg, Germany

ABSTRACT

In the age data digitalization, important applications of optics and photonics based sensors and technology lie in the field of biometrics and image processing. Protecting user data in a safe and secure way is an essential task in this area. However, traditional cryptographic protocols rely heavily on computer aided computation. Secure protocols which rely only on human interactions are usually simpler to understand. In many scenarios development of such protocols are also important for ease of implementation and deployment. Visual cryptography (VC) is an encryption technique on images (or text) in which decryption is done by human visual system. In this technique, an image is encrypted into number of pieces (known as shares). When the printed shares are physically superimposed together, the image can be decrypted with human vision. Modern digital watermarking technologies can be combined with VC for image copyright protection where the shares can be watermarks (small identification) embedded in the image. Similarly, VC can be used for improving security of biometric authentication.
This paper presents about design and implementation of a practical laboratory experiment based on the concept of VC for a course in media engineering. Specifically, our contribution deals with integration of VC in different schemes for applications like digital watermarking and biometric authentication in the field of optics and photonics. We describe theoretical concepts and propose our infrastructure for the experiment. Finally, we will evaluate the learning outcome of the experiment, performed by the students.

Keywords: Education, Optics and Photonics Applications, Visual Cryptography, Digital Watermarking, Biometric Authentication, Active Learning

1. INTRODUCTION

As data digitalization has been growing rapidly since last few decades, awareness of information security and privacy is much needed in the field of optics and photonics. Biometrics and image processing are important applications of optics and photonics based sensor technologies where it is essential to protect the data and the privacy of individuals. However, security protocols used in those technologies can be very complicated and not easy to teach for educational purposes. A student in optics education may come from different background as theoretical physics, engineering, electronics, laser science, media technology, etc. and may not have the necessary background in information security. Hence, it would be helpful for the students if we can introduce some simpler security techniques rather than complex ones. Visual cryptography (VC) is a human interaction based encryption technique on images (or text) where decryption is possible with human eyes. VC technique is identified as a secret sharing scheme. In this technique, participants get encrypted image shares and when the image shares are physically superimposed together, the original image can be decrypted with human eyes. This human-interaction based security technique is simple to understand and has a wide range of applications in optics and photonics. For example: VC technique can be used to improve the security and privacy of copyright protection of images by embedding watermarks[4-7] or biometric authentication[8-10]. In this paper, we present about the design and development of a laboratory experiment where students can actively learn in a collaborative manner. Specifically, the laboratory experiment introduces concepts of VC and its application in image watermarking and biometric authentication to raise the awareness of information security in optics or media education.

The rest of the paper is organized as follows. In section 2, we highlight related works in field of VC and its applications to biometric privacy and copyright protection. Some theoretical background to basic VC scheme and model are given in section 3. Section 4 and 5 discuss about educational objective and description of the experiment. Section 6 provides the evaluation and learning outcome. Finally, we conclude our paper in section 7.

* avikarsha.mandal@hs-offenburg.de; phone 0049 781 205-4683

Optics Education and Outreach IV, edited by G. Groot Gregory, Proc. of SPIE Vol. 9946, 99460X
 · doi: 10.1117/12.2237923

2. RELATED WORKS

The concept of VC was first introduced by Naor and Shamir[1] in 1994. They proposed a visual secret sharing (VSS) scheme where a black and white secret image can be encoded into *n* shares. These shares can be printed on transparencies individually and distributed among *n* participants. The decryption of the secret image is only possible when *n* participants stack up their own transparencies together, whereas *n-1* shares reveal no information about the secret image. This scheme is known as *n* out of *n* VSS scheme. This scheme can be extended to *k* out of *n* VSS where stacking any *k* transparencies together reveals the secret image[2]. Ateniese et al. proposed the general access structure of VC[3]. Recently, a book[11] by Weir et al. gives an extensive overview of VC schemes and its application in different domains. Different approaches to integrate VC in copyright protection schemes can be found in previous literature [4-7]. Cimato et al.[7] has provided a general model for watermarking scheme with VC. Some works about biometric authentication schemes using VC technique are there in the literature[8-10].

3. THEORATICAL BACKGROUD

3.1 Basic 2 out of 2 scheme

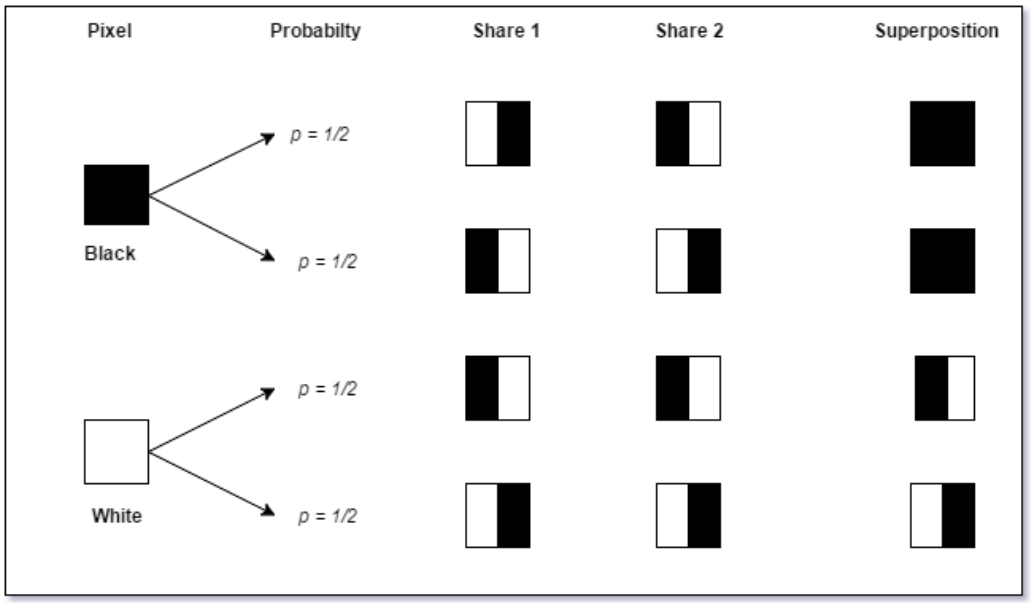

Figure 1: 2 out of 2 VSS with 2 subpixels

The simplest way to understand Naor and Shamir's *n* out of *n* VSS scheme is to consider $n = 2$. This basic 2 out of 2 VSS scheme with 2 subpixels is shown in Figure 1. We can consider a black and white secret image (binary) *S* which has total *m* pixels. Now, a dealer can create two binary black and white shares S_1 and S_2 by encoding every single pixel of secret image *S*. If the pixel of *S* is black, the dealer randomly chooses (flipping a coin) one of the first two rows of Figure 1. In the same manner, if the pixel *p* is white, the dealer randomly selects one of the last two rows of Figure 1. Notice, in the case of 2 out of 2 VSS with 2 subpixels each share created by the dealer contains twice more pixels than original image *S* i.e. total $2m$ pixels as for each pixel from the image *S*, associated pixels in S_1 and S_2 are two.

From the security perspective, the pixel selection from the dealer is randomly done and probabilities are same for both cases for shares S_1 and S_2. Hence, an attacker looking at a single share cannot able to tell if the secret pixel is black or white. Therefore, this scheme gives us perfect secrecy. At the rightmost column of the figure 1, we can see the results when two participants stack their two shares together. If original secret pixel is black, two black subpixels will appear and if original secret pixel is white, one white subpixel and one black pixel will appear. However, the human visual system will able be differentiate whether the original pixel was black or white. The reason is that the merged two black subpixels will appear black and merged black and white subpixels will appear gray due the contrast between white and black subpixels[1]. In this process, the participants can decrypt the whole secret image with their eyes by stacking their shares properly. An example of 2 out of 2 VSS with 4 subpixels is shown in Figure 3.

3.2 VC Model

In this section, we explain the mathematical model behind VC. The secret image here is basically a collection of black and white pixels. Now, the secret image is divided into *n* shares (transparencies) i.e. each pixel appears one for each share. Furthermore, each share is divided into *m* subpixels (black and white). The shares can be represented by *n* x *m* Boolean matrix $S = [s_{ij}]$, where

$$s_{ij} = 1, \text{ iff } j^{th} \text{ subpixel of } i^{th} \text{ transparency is black}$$

$$s_{ij} = 0, \text{ iff } j^{th} \text{ subpixel of } i^{th} \text{ transparency is white}$$

This matrix representing the shares is known as *distribution matrix*[7]. For example, the distribution matrix for 2 out of 2 VSS scheme with 2 sub-pixels is as follows:

- Black pixel: $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ or $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$
- White pixel: $\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$ or $\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$

Pixel expansion and contrast are two important parameters in any VC scheme. When the participants stack their shares i_1, i_2, . . . , i_r, together to reconstruct the secret image, the gray level of the combined share is directly proportional to Hamming weight *w(V)* of *m* vector *V=OR(*rows of shares $i_1, i_2, \ldots, i_r$ *).* Our human eye interprets this gray level with some rules of contrast and decides if the pixel is black or white. This superposition of the pixels is basically an OR operation. Some VC scheme[6] uses XOR operation for improvement of the reconstructed image but then human visual system cannot perform the decryption anymore. More details about VC model can be found in the literatures [3, 7, 9].

4. EDUCATIONAL OBJECTIVE

The main educational objective of our experiment is to provide awareness of information security in optics or media education and improve learning experience. In Offenburg University, we teach 'Practical IT Security' in Bachelor for media engineering students. The course comes with theoretical lectures along with practical laboratory exercise session. During the past few years, we observed some students often face difficulty while performing IT security related exercises. We have discussed this issue with the students during the feedback session. The main factors impacting the performance of the execution are observed as follows:

i) Some student lacks some basic understanding of IT security and programming skills. It can be difficult for the students if the exercises involve a good amount of computer aided computation.

ii) It would be more encouraging for the students if the IT security exercises have some practical implication on applications in their respective field of studies.

iii) Effectiveness of task execution degrades with individual learning.

To improve the learning experience, we decided to implement a new laboratory exercise considering aforementioned factors. Our choices for developing a laboratory experiment based on VC are threefold. First, introducing the concept of VC could eliminate the factor i) as VC schemes rely on human interaction. As we provide the script to perform VC, a student could focus on understanding the concept rather than doing complex programming. Second, we can integrate VC into some applications of media and optics to eliminate factor ii). Image copyright protection is an important area in media studies, whereas biometrics is an integral part of optics. To handle the factor iii), we can model our experiment with collaborative learning [12] and active learning[13] where a student can actively participate with collaboration with fellow students.

5. EXPERIMENT DESCRIPTION

The design, implementation details and proof of concept of the practical laboratory experiment are described in this section. There are three parts of the experiment that students have to perform: i) Realization of visual cryptography, ii) Digital watermarking with VC technique and iii) Biometric authentication with VC technique. It is important for the students to prepare themselves prior to the experiment with a provided instruction manual. The manual describes the

necessary theoretical basis, experimental infrastructure and execution instructions of the experiment. Students can access the instruction material for this exercise from our e-learning platform.

5.1 Realization of Visual Cryptography

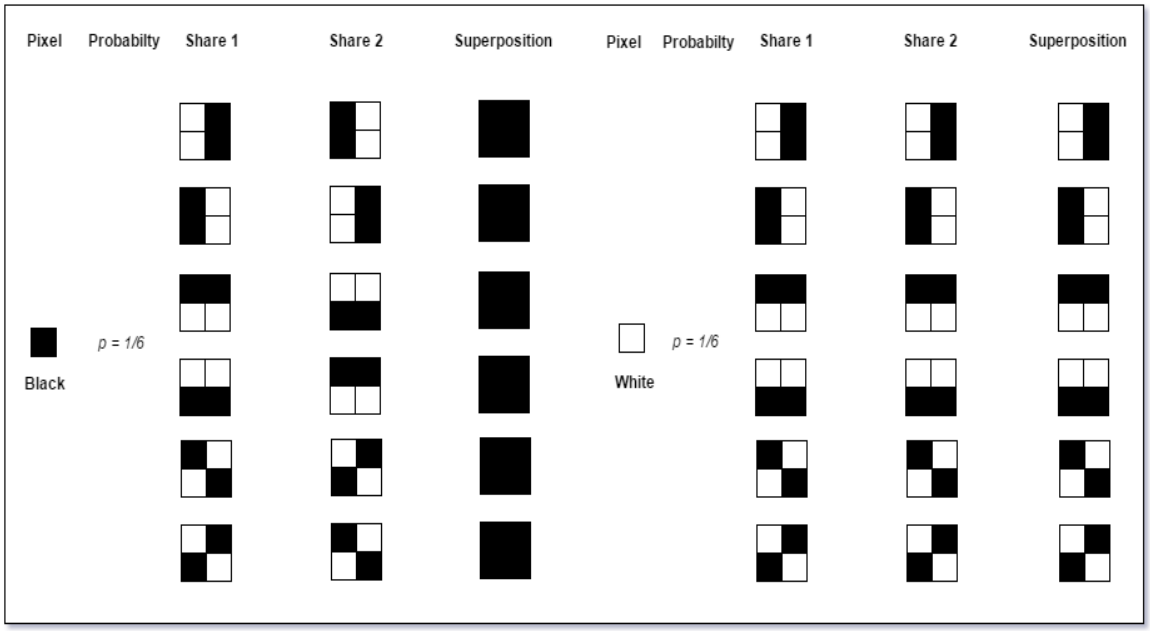

Figure 2: 2 out of 2 VSS with 4 subpixels

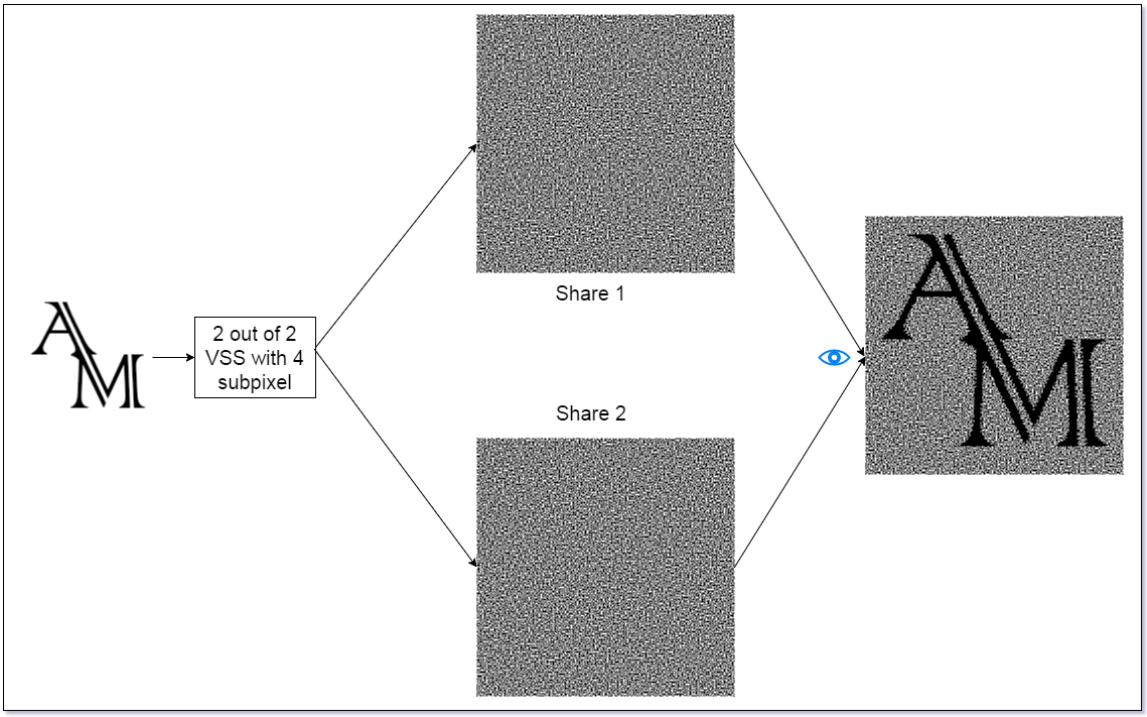

Figure 3: Example of 2 out of 2 VSS with 4 subpixels

First part of the experiment is a realization of visual cryptography. In this exercise, students will learn the concepts of VC technique with a practical hands-on experience. We have implemented a script which performs the basic 2 out of 2 VSS scheme in the python programming language for this exercise. Our implementation uses python image processing library (PIL) for different image processing features. The implementation of basic 2 out of 2 VSS is done with 4 subpixels. The reason for choosing 4 subpixels over 2 subpixels is to maintain the aspect ratio of the original image. As from Figure 1, we can see the pixel expansion is 2. Hence, it could create a stretching of the original image horizontally and may cause some distortion. To avoid this, we can associate each pixel of the original image to a block of (2 x 2) i.e. 4 subpixels as illustrated in Figure 2.

The rules of encryption and decryption process are shown in Figure 2 and the idea is same as explained in section 3.1. Each share should have 2 white sub pixels and 2 black subpixels. Therefore, we can have 4C2 i.e. 6 possible combinations. We encode with the same pattern for both shares if the original pixel is black and use opposite pattern if the original pixel is white as shown in Figure 2. The implemented code of 2 out of 2 is VSS is provided to students to perform this exercise. The students can be divided into groups where each group consists of two members. Students can choose any black and white image as an input to the algorithm. For example, of an execution of this exercise is depicted in Figure 3. A binary logo with size 128 x 128 pixels is given as an input to the algorithm. The script will output two binary image shares of size 256 x 256 pixels. Now, each student in the group receives one share and print out on a transparent paper. A student can realize his individual share indeed filled with random pixels and gives no information of the original logo. To decode the original logo, each student has to collaborate with his group mate. When both students stack their transparencies together in front of a light source, the original logo will be visible as shown in Figure 3.

5.2 Digital Watermarking with VC

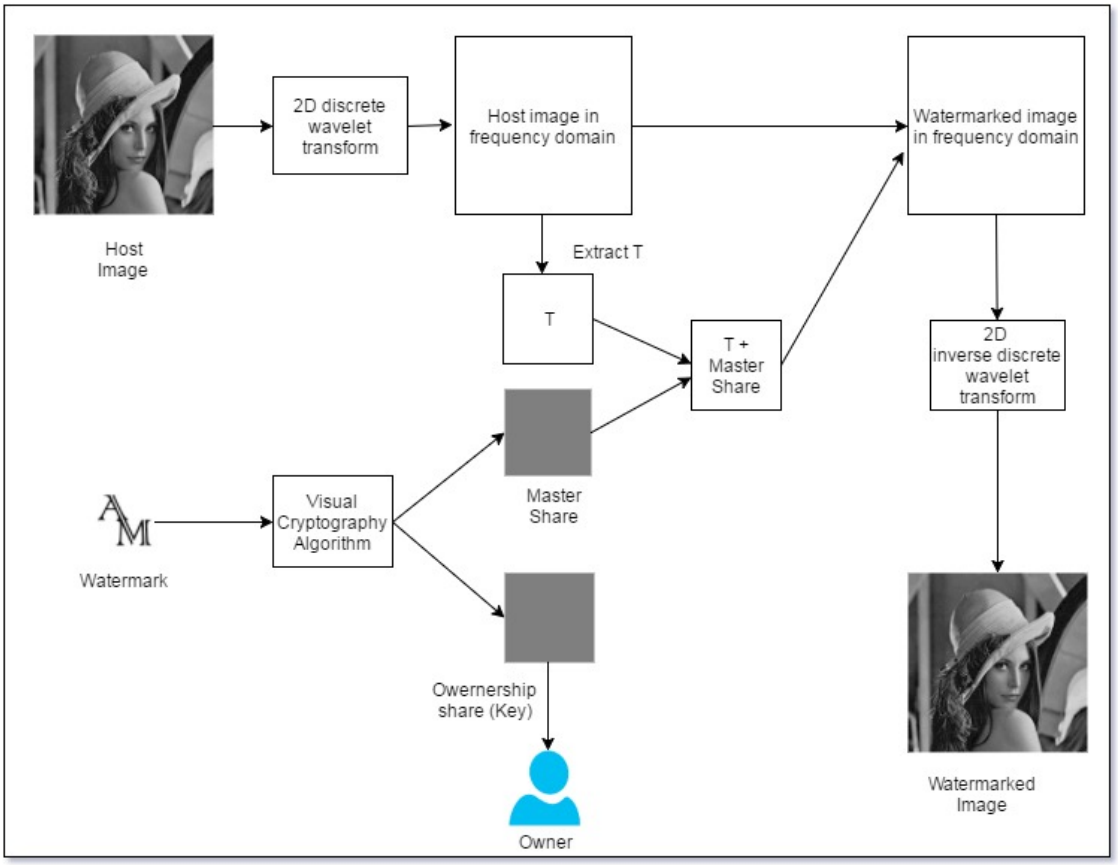

Figure 4: Watermark embedding phase

Second part of the exercise deals with integration of VC in a digital watermarking scheme. Digital watermarking is a technique used for protecting the copyright of any digital media such as images. Watermarks are basically some digital information (Ex: logo) about the owner. Usually watermarks are embedded into images, and extracted when the owner

wants to claim his copyright of the image. Currently, many of the watermarking processes are done with transfer domain techniques like discrete wavelet transform (DWT)[4,6] for better security and robustness.

There are two phases of this exercise: i) watermark embedding phase and ii) watermark extraction phase. In our implementation, we have used numpy and pywt packages of python along with PIL library. The implementation uses a VC based watermarking technique proposed by Hsu et al.[4] and can perform watermarking without a trusted third party. During the embedding phase, a watermark logo can be split with 2 out of 2 VSS. Owner of the host image keeps one of the shares (key) and other (master share) being embedded into the host image in the frequency domain. During the extraction phase, owner can extract the master share from the watermarked image and superimpose with his ownership share to get the watermark.

An illustration of the process involved for watermark embedding with VC is shown in Figure 4. Here, imagine a student would like to embed his own binary watermark *W* of size 128 x 128 into a gray scale host image *H* of size 512 x 512. The student can split the watermark *W* in two shares with 2 out of 2 VSS scheme like in the previous exercise. Each share will have a size of 256 x 256. Out of two, he will use the master share for embedding purpose and ownership share for watermark extraction. On the host image *H*, he can execute a 2D Haar wavelet transform to convert it into the frequency domain. Then, a square *T* of size 256 x 256 is extracted starting from any arbitrary point of the host image in frequency domain and divided into non-intersecting blocks of 4 x 4. Now, each block of T will have 4 wavelengths co-efficient and each block can be modified according to blocks of master share. After that, the modified T is integrated into the host image in the frequency domain at the specific location where it was before. Finally, the student can perform a 2D inverse Haar wavelet transform to get watermarked image. In Figure 4, we can see there is no major difference in quality between the resulted watermarked image and the host image.

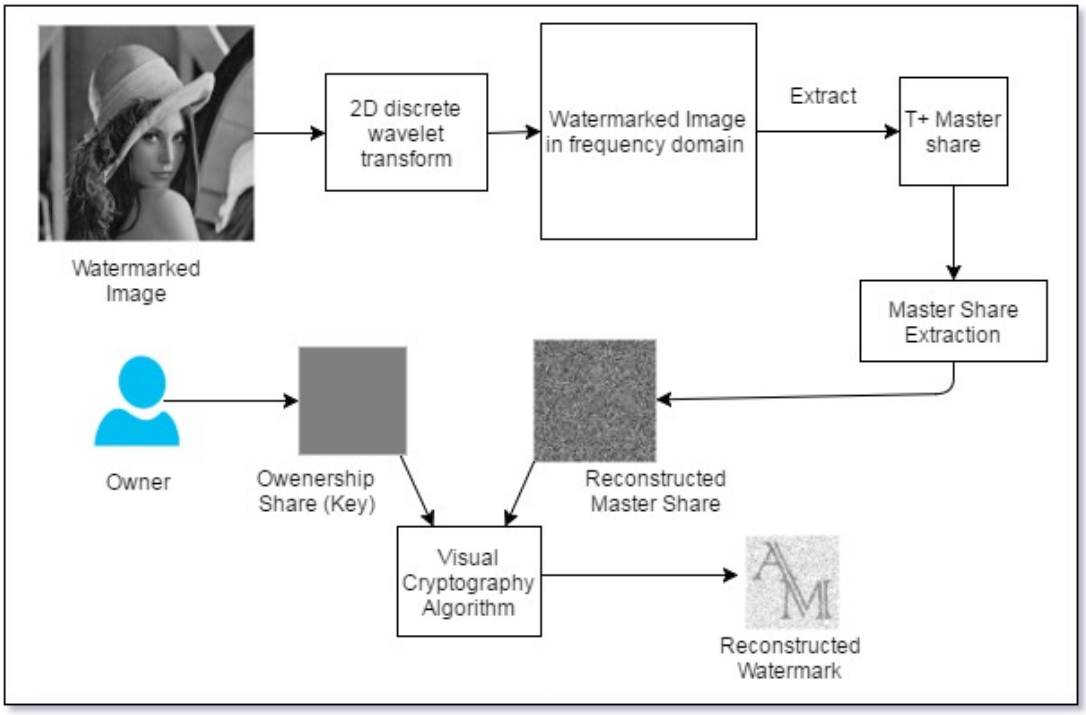

Figure 5: Watermark extraction phase

The process involved during watermark extraction phase is depicted in Figure 5. The watermarked image is again processed through 2D Haar wavelet transform to extract the modified T. Then, the master share can be reconstructed from modified T according to wavelet values of original T. Finally, a student can stack the reconstructed share and his ownership share to get the watermark and prove his ownership of the image. Comparing watermarks in Figure 5 and 4, we can observe that there is minor quality deterioration in the result of the reconstructed watermark from the original watermark.

5.3 Biometric Authentication with VC

Final part of the experiment is the application of VC in biometric authentication. The goal of this part is that the students should realize how VC could help to protect privacy of biometric data in biometric authentication. The idea is this exercise is inspired from the approach proposed by Ross et al.[8]. A usual biometric authentication system compares feature set of raw biometric data (Ex: probe fingerprint) against feature set of biometric templates (Ex: Enrolled image) stored in a central database to verify the identity of a person. However, the privacy of the biometric data can be violated by the owner of the central database. This problem can be prevented by using VC where an enrolled biometric image can be split among different databases. Hence, the database owner can not reveal the original image with his single share.

Figure 6 presents the scheme for biometric authentication with VC exercise. There are two phases of this exercise: i) Enrollment phase, ii) Authentication phase. As the feature extraction from biometric template is quite complex and computer aided process, for simplicity, students are instructed to verify the templates with their visual system. We have downloaded some visually distinguishable fingerprint images from NIST fingerprint database[14]. As these images are in gray scale, we converted them into binary. To execute this exercise, we have adopted a collaborative learning approach[12]. Students are divided into several groups, consisting 5 or more members in each group. In a specific group, students are allotted with different tasks. For example: one student (student *A*) can act as a trusted third party, two students (student *B* and *C*) are database owners and the rest of the students (student *D*, *F* . . .) want to claim their identity in the biometric system. First, we distribute different fingerprint images to the students (*D*, *F*. . .) and imagine their fingerprint image represents their identity. During the enrollment phase, *D* gives his image to the trusted third party (student *A*) to enroll in a biometric system. However, student F does not enroll to student *A* but still willing to get accepted by the biometric system. Now, *A* can apply 2 out of 2 VSS scheme to fingerprint of *D* and gets two shares. Thereafter, *A* sends share 1 to database 1 (owner *B*) and share 2 to database 2 (owner *C*) to enroll *D* into the system. Hence, *B* cannot reveal the fingerprint of *D* from his share 1 as he will see some random pixels and same applies to *C*.

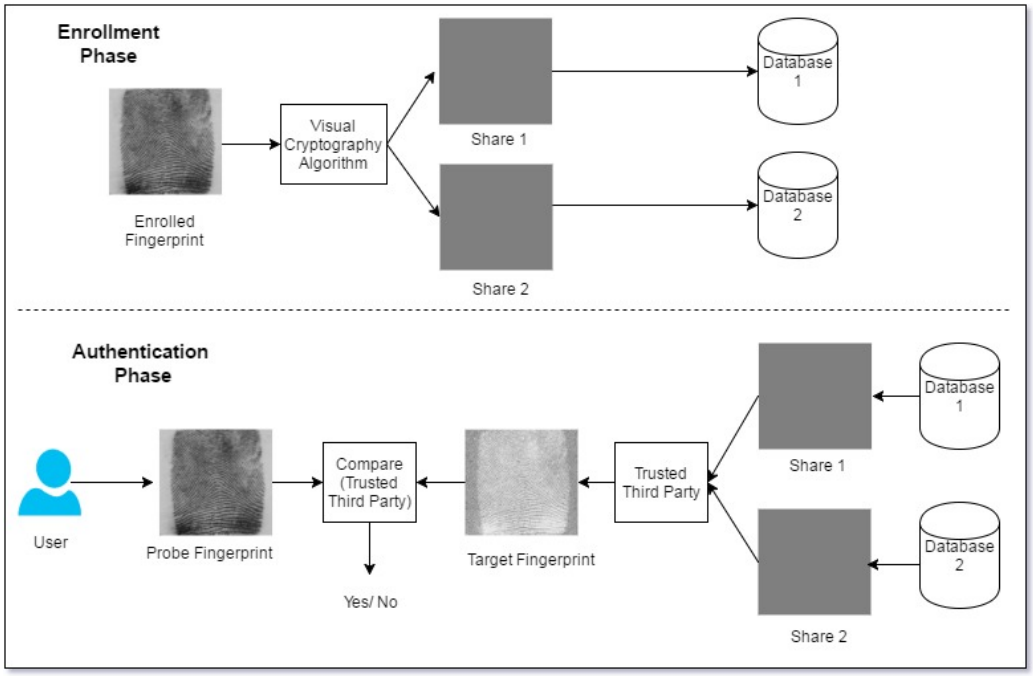

Figure 6: Scheme for Enrollment and Authentication for fingerprint image

During the authentication phase, *D* and *F* send their fingerprints (probe fingerprint) to *A* in order to get identified in the system. Now, A can make a request to *B* and *C* to send their shares from their database. When *A* receives both shares, he can stack the images together to get the target fingerprint. Finally, A visually compares the target fingerprint with the probe fingerprints from *D* and *F*. As *D*'s probe fingerprint matches with target fingerprint, *D* gets accepted in the biometric system and *F* fails to get accepted.

6. EVALUATION AND LEARNING OUTCOMES

The proposed laboratory experiment will be in operation for media engineering students for the upcoming winter semester 2016-17. We have conducted a laboratory session to test the preliminary version of the experiment with few participants. The participants were mainly students and employees of Offenburg University from different educational backgrounds. The candidates were perfectly suitable for the experiment evaluation purpose as their expertise does not belong to IT security domain. Before the experiment, we have explained some theoretical basis for the exercises to the participants and distribute our implemented python script with the instruction manual. We were also present there in order help the participants if they have any questions. Majority of them were very enthusiastic and discussed different concepts in an interactive way. All participants were able to perform all three parts of the experiment successfully. At the end of the session, we distributed some evaluation questionnaire to get some feedback. Most of the participants (60%) found this human interaction based technique was helpful and 20% very helpful on a scale of 1 to 6, ranging from useless to very helpful to create awareness of information security. They also found that the hands-on experience with collaboration was effective to have a deeper understanding on this topic. The majority of the participants voted for the biometric authentication with VC as the most interesting part the experiment and found the overall experience positive.

7. CONCLUSION

We have demonstrated how visual cryptography can have an impact on teaching in media education. It is easy to use and awareness of information security can be conveyed with a hands-on experience. Students can learn and realize the concepts with our designed laboratory experiment. Furthermore, collaborative learning can help students to improve the execution of the experiment. Currently, we have tested a preliminary version of the experiment with a limited number of participants. The better understanding of learning outcome can be obtained when we will have a larger pool of participants in the upcoming semester. We are flexible to adjust the experiment based on their feedback if it is necessary.

REFERENCES

[1] Naor, M. and Shamir, A., "Visual Cryptography," Advances in Cryptology: Eurpocrypt'94 Lecture Notes in Computer Science Vol. 950 Springer Berlin, 1-12 (1995).

[2] Verheul, E.R. and Van Tilborg, H. C., "Constructions and properties of k out of n visual secret sharing schemes, " Design Codes and Cryptography 11(2), 179-196 (1997).

[3] Ateniese, G., Blundo, C., De Santis, A. and Stinson, D.R., "Visual cryptography for general access structures," Information and Computation 129(2), 86-106 (1996).

[4] Hsu, C. S. and Tu, S. F., "Digital watermarking scheme with visual cryptography," In Proceedings of the International Multi Conference of Engineers and Computer Scientists IMECS (Vol. 1), (2008).

[5] Hsu, C.S. and Hou, Y.C., "Copyright protection scheme for digital images using visual cryptography and sampling methods," Optical Engineering 44(7), 077003 (2005).

[6] Lou, D. C., Tso, H. K. and Liu, J. L., "A copyright protection scheme for digital images using visual cryptography technique, "Computer Standards & Interfaces 29(1), 125-131 (2007).

[7] Cimato, S., Yang, J.C.N. and Wu, C.C., "Visual cryptography based watermarking: definition and meaning," In International Workshop on Digital Watermarking, Springer Berlin Heidelberg, 435-448 (2012).

[8] Ross, A. and Othman, A., "Visual cryptography for biometric privacy," IEEE transactions on information forensics and security 6(1), 70-81 (2011).

[9] Monoth, T. and Anto P, B., "Tamperproof transmission of fingerprints using visual cryptography schemes," Proc. Comput. Sci. 2, 43-148 (2010).

[10] Revenkar, P. S., Anjum, A. and Gandhare, W.Z., "Secure iris authentication using visual cryptography," Int. J. Comput. Sci. (IJCSIS) vol. 7 no. 3, 217-221 (2010).

[11] Weir, J. P. and Yan, W., [Visual Cryptography and its applications], Ventus Publishing ApS (2012).

[12] Dillenbourg, P., "What do you mean by collaborative learning," Collaborative-learning: Cognitive and computational approaches 1, 1-15 (1999).

[13] Prince, M., "Does active learning work? A review of the research," Journal of engineering education 93(3), 223-231 (2004).

[14] Flanagan. P., "NIST 8-Bit Gray Scale Images of Fingerprint Image Groups(FIGS)," NIST, 19 April , 2016, http://www.nist.gov/srd/nistsd4.cfm (30 july 2016).