REVIEW OF BIOMETRIC PRIVACY USING VISUAL CRYPTOGRAPHY

Anix Jugal D'Cunha, Tahir Naquash

Department of CSE,
AIET, Mijar,
Karnataka, India

Abstract: **Authentication is done using Biometric, which are user friendly. Biometrics are used to collect some raw biometric data and then data compares with the data stored in database for providing access. It is easy for attackers to attack the data stored in database. Hence security is very necessary for biometrics. Physical and behavioral are the 2 features of Biometrics. To protect Biometrics data from the various attack is the main purpose of this paper. The authorized person send and receive the data with the required keys using visual cryptography which is the secret communication of the images with authorized persons.**

Keywords: **Balanced Block Replacement (BBR), Extended Visual Cryptography (EVC), Cover Images, Gray Scaling, Rescaling, Transparencies Secret Image.**

1. INTRODUCTION

"Visual Cryptography for Biometric Analysis" is used to identify a person which matters a lot nowadays, under which security is provide for the images. Therefore, sending and receiving the images are secured by using this analysis.

2. PURPOSE

Any authenticated person can read a data when a data is transmitted over a network. In order to avoid this we encrypt the data and send it to required intended person in which the receiver will encrypt the data and uses it. Perfect secrecy is the main intention of visual cryptography.

3. PROPOSED

We make use of Secret image and a cover image in this particular analysis, where both are overlapped with each other. We can only access the secret image when 2 cover images are available simultaneously. By only 1 cover image it is not possible to share any data about the secret image. In order to perform this we use "Floyd Steinberg Error Diffusion" and "BBR" algorithms.

4. EXISTING SYSTEM

Biometric templates are protected using cryptography. Only the authorized sender or the receiver can encrypt or decrypt the messages which has been shared. Intended receiver (authorized receiver) can decrypt and encrypted message and read it using some mathematical process. Visual information is encrypted using VCS technique such that the decryption process can be done by the human visual systems. Using this technique the biometric data (e.g. image) is captured from the authorized user. This original image is divided into the two cover images and, then each cover image is stored in two different databases geographically apart. When both the cover images are simultaneously available then only we can access that original image. So the size of the original image becomes larger instead of original size this is the disadvantage of the existing system and we are providing a solution for this.

5. PROPOSED SYSTEM

Both secret image and cover images should be of the similar size in cryptography. Visual cryptography is used even if the images are of different size. Hence the bug is countered. Different sheet images are encode with a secret image using VCS, each having no information about the original image, which have random set of pixels. Hence the new framework i.e., extended VCS is used to get a curiosity of an interceptor by giving the existence of a secret image.

The images are converted to binary images using halftone algorithm. Extended visual cryptography and visual cryptography is used to preserve the image size of an halftone image which is created.

Rescaling method was used to solve the problem of larger size of the images which use to appear in terms pixel resolution. Visual cryptography works on the black and white images and images of fix size. If the image size is more we use rescaling method to fix the size of an image.

The color images are converted into grayscale images. As visual cryptography only works for the black and white images.

We use Digital Halftoning Method to define our own palate to printer palate in order to print maximum number of shades. Every pixel value should be nearer to palate value. Every quantization error should be removed using error diffusion method. Quantization error is distributed to neighboring pixels using the process of halftoning.

In order to avoid the pixel expansion during hiding the original image into cover image we make use of Balanced Block Replacement (BBR).The pixels in white or black color is placed in certain combinations.

We use pattern matching technique to check a given set of tokens in the presence of constituents of some patterns. The secret image is compared with image stored in database when we access it. If comparison matches then only we can access the secret image.

5. ADVANTAGES

1) No Pixel Expansion The size of original image is as it is.
2) High Level Security for biometric privacy.
3) Prevent Attacks of biometric images.
Secure Databases

6. DRAWBACKS

When we apply visual cryptography in the existing system, the pixel expansion occurs resulting in the increased size of original image.

7. Software Tools

7.1 Software Requirement

1) Operating System - Windows 7/8
2) Application Server - Apache Tomcat 7.0.34
3) Front End - HTML, Java, Jsp, Css
4) Scripts - JavaScript
5) Server side Script - Java Server Pages
6) Database - MySQL
7) Database Connectivity - JDBC

7.2 Hardware Requirement

1) Personal computers with required Configuration.
2) Biometrics kit to fetch human biometric data and transform it into a image.

8. Conclusion

Thus we have studied to protect the privacy of a image database by decomposing an input private image into two independent sheet images such that the private image can be reconstructed only when both sheets are simultaneously available. The proposed algorithm selects the host images that are most likely to be compatible with the secret image based on geometry and appearance. Increasing the pixel expansion factor can lead to an increase in the storage requirements for the sheets. In the recent literature there have been some efforts to develop a VCS without pixel expansion. But no such scheme currently exists for generating sheets that are not random noisy images. Thus, more work is necessary to handle this problem.

References

[1] Pardhasaradhi, P.Seetharamaiah, "A Rumination of Error Diffusions in Color Extended Visual Cryptography", *International Journal of Computer Trends and Technology (IJCTT) – volume 15 number 1 – Sep 2014,ISSN: 2231-5381.*

[2] N. Askari, H.M. Heys, and C.R. Moloney, "AN EXTENDED VISUAL CRYPTOGRAPHY SCHEME WITHOUT PIXEL EXPANSION FOR HALFTONE IMAGES", IEEE Canadian Conference Of Electrical And Computer Engineering (CCECE), 2013 26th.

[3] Dr.V.R.Anitha, Dilipkumar Kotthapalli, "Extending the Visual Cryptography Algorithm Without Removing Cover Images", *International Journal of Engineering Trends and Technology (IJETT) - Volume4Issue4- April 2013,* ISSN: 2231-5381.

[4] Arun Ross, Asem Othman, "Visual Cryptography for Biometric Privacy", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 6, MARCH 2011.