VISUAL CRYPTOGRAPHY FOR BIOMETRIC PRIVACY

***Project Reference No.:** 45S_BE_1566*

***College** : Mangalore Institute of Technology and Engineering, Moodbidri*
***Branch** : Department of Electronics and Communication Engineering*
***Guide(s)** : Mr. Ganesh V N*
***Student(S)** : Ms. Suprabha*
Mr. M B Sachin
Mr. Shravan Kumar
Mr. Sooraj Shetty

Keywords:

Biometrics, Visual Cryptography, VCS, Private Face Image

Introduction:

In today's fast-moving world, security plays a vital role in everyday life. Today, many digital documents (images) are distributed and traded online. Security has become an important factor in communicating, this is due to the presence of hackers waiting for an opportunity to gain access to private data.

Biometrics is the measurement of characteristics that can be used to identify an individual. There are a variety of applications that need to be identified such as computerized control login, secured electronic banking, border crossing, airport, mobile phones etc. The biometric system works on retrieving raw biometric data from the user, extracting the set of features from the data and comparing it with the templates stored on the database to verify the desired identity. The template data is created during enrolment and is mostly stored along with the original data. This increased the need for confidentiality in the article by adequately protecting the content of the website. Hence, we use "Visual Cryptography". Image secret share creation for RGB images was introduced by Naor, M. and Shamir, A. (1995) based on features of semigroups. Arun Ross, Asem Othman (2011) says that an image is bifurcated into two shares to be displayed only when these two shares are available together; photos of individual hosts won't reflect the identity of the original image. Jeng-Shyang Pan, Tao Liu, Hong-Mei Yang, Bin Yan, Shu-Chuan Chu, Tongtong Zhu (2021) in RGB image method, the encrypted shares are removed from the stack image and matched with the original image. Decryption and encryption are done with the Blowfish Algorithm. M. Karolin and T. Meyyappan (2019) gives the idea about the Visual Cryptographic technique while transferring images. RGB image, shares encrypted and decrypted to stacked image and then same as the original image. M. Karolin, Dr. T. Meyyappan (2015) says during the encryption phase the real image collapses into three shares this can be done with a large amount of future production sharing for security enhancement. This paper uses a VC for color images in a biometric application.

Objectives:

1. The main objective of this study is to increase security in communication by encrypting the information using a key that is created through using a data.

2. The process Visual Cryptography encrypts a private image into stocks so that it can collect a sufficient number of shares produces a private image. This project uses VC of colored images in a biometric application.
3. The need of reliable and effective security mechanisms to protect information systems is increasing due to the rising magnitude of identity theft in our society.
4. More secured images can be decrypted using this idea and get a better image quality.

Methodology:

The two stages of biometric system are registration and recognition. The first step involves extracting the feature and pre-processing. The features are stored as templates on the database.

- Working

The proposed method is divided into 2 categories, namely Image Encryption and Decryption. Here we use Halftoning “Floyd Steinberg Dithering Algorithm” for image capture and Blowfish Algorithm to protect against illegal attacks and work faster than printed algorithms and keep the algorithm strong. The dithering algorithm is used instead of image stabilization. The potency of the actual image is maintained by this method.

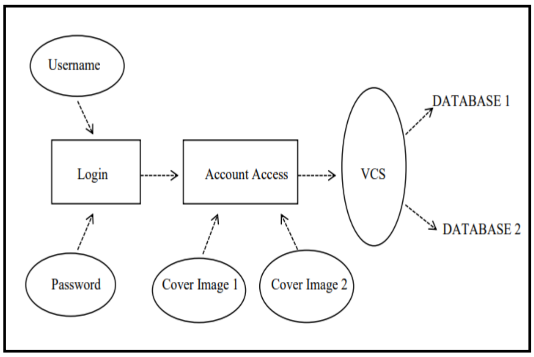


Fig 1: Data Flow diagram for the Proposed System

- Encryption

Every image consists of 3 shares, RGB, hence here we divide each image into 3 shares as shown in Fig. 2.2. This is known as Sieving. XOR- based VC method is used to generate shares. These RGB shares are divided into 2 more shares each i.e., R1, G1, B1, R2, G2, B2 a total of 6 small shares. This is called Division. Further these 6 shares are shuffled. This is called Shuffling. Then a random share is generated to form 2 different shares and saved, these are then shared to different users or database. This is called Combining.

- Decryption

The 2 randomly generated images are chosen to obtain the decrypted image i.e., the original image as shown in Fig. 2.3. Next process is face recognition/matching, where it matches the original image with the decrypted image and checks for the similarity.

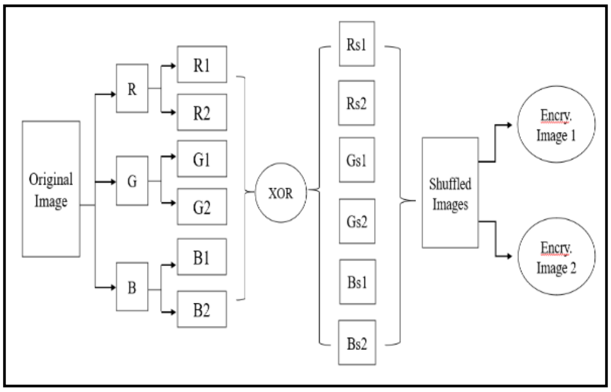


Fig 2: Encryption method

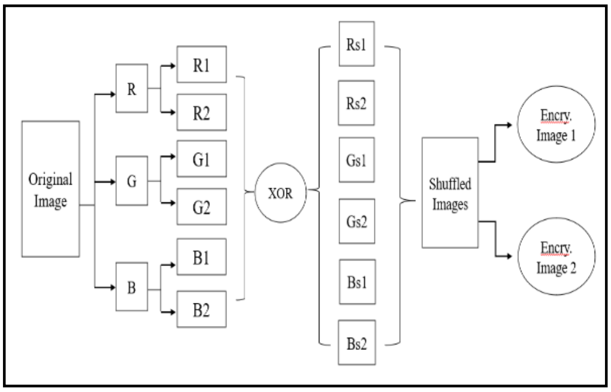


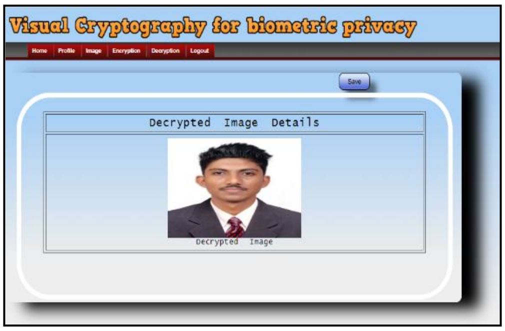
Fig 3: Decryption method

- Face Matching

After the encryption and decryption process, verification of the image is necessary. This is done through RANSAC method. It is used to detect the face edges which is helpful for the detection and face verification process.

Conclusion:

VC is basically an encryption method which has a merit of decrypting encrypted images rather than cryptographic computations. There are many techniques in biometric that are available such as fingerprints, retina, face, iris, palmprint, voice, signature, keystroke and facial thermogram etc. The significance of VCS in enhancing in the security and integrity of secret information has also been considered. The work has a better than image quality.


Visual Cryptography for biometric privacy

Decrypted Image Details

Decrypted Image

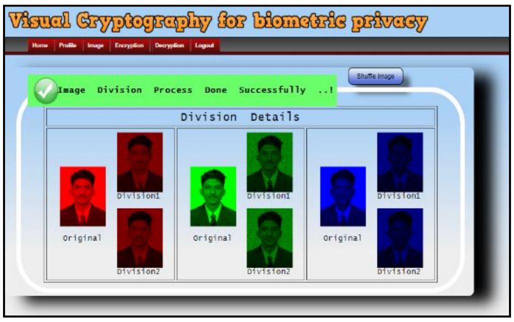

Visual Cryptography for biometric privacy

Image Division Process Done Successfully ..!

Division Details

Original
Division1
Division2
Original
Division1
Division2
Original
Division1
Division2

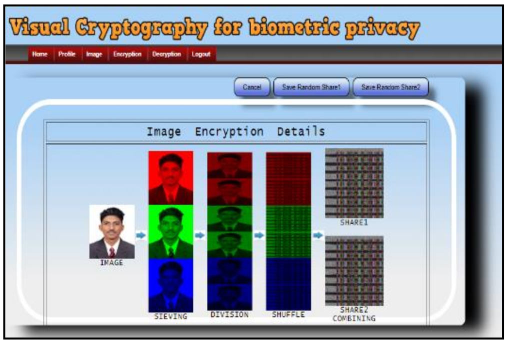
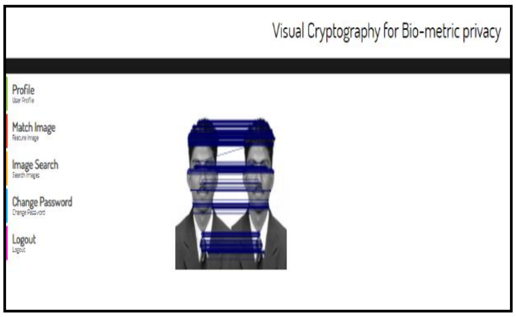

Visual Cryptography for biometric privacy

Image Encryption Details

IMAGE
SIEVING
DIVISION
SHUFFLE
SHARE1
SHARE2
COMBINING


Visual Cryptography for Bio-metric privacy

Scope for future work:

Visual cryptography seems to be simple, but these flaws appear to be a threat in bringing out the entire magnificence of visual cryptography. The contrast loss must be minimized or eradicated to achieve such a high accuracy. The major concern due to pixel expansion is the requirement of storage space. A VC scheme utilized must be efficient such that it brings about very low contrast loss and pixel expansion. This has received little attention so far as it requires complex models and faster resources. It is necessary that further research be conducted in this direction. Deep learning in biometrics has been explored very little beyond common traits like face, fingerprints, iris and voice. However, very few behavioral biometric traits have been explored using deep learning approaches. We would explore more such applications of deep learning, which hold a lot of potential in the field of biometrics to secure real-world applications.