International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-3, Issue-1, January 2015

Securing and Secrete Image Sharing Using Visual Cryptography Scheme

Rupali Lambe, Mayuri Ghadge,Tai Ingole, Pratiksha Surwase

Abstracts-**To verify identity of person his /her physical or behavioural characteristics can be use,this strategy is called as Biometrics. Preservation of privacy of digital biometric data such as iris,face images etc. which stored in central database becomes more essential. This paper introduced the new visual cryptographic technique that allows encryption of visual information such that decryption can perform using human visual system hence cryptography computation does not required any extra hardware and software. In visual cryptography secrete image is encrypted into number of shares which independently can not reveal information about original image. For getting information about original image all sheets must be available simultaneously.**

Keywords- **Encryption,Decryption,Biometrics,Shares, Sheets.**

I. INTRODUCTION

A .Biometric

Biometric is defined as science of establishing identity of individual based on physical and behavioral characteristics . Since each one to have unique biometric if this biometric data is modified it is not possible to replaced it[2].

B. Cryptography

Cryptography and data hiding this two methods are used for protecting data and providing security to important information. For transmitting data in secure way it convert data into unreadable format or secret code, cryptography and watermarking are most popular method for data hiding.

Manuscript received January 25, 2015.

Rupali Lambe, Student at Savitribai Phule Pune University,Department of Computer Engineering,Shri Chhatrapati Shivaji College Of Engineering Shrishivajinagar.

Mayuri Ghadge, Student at Savitribai Phule Pune University,Department of Computer Engineering,Shri Chhatrapati Shivaji College of Engineering ,Shrishivajinagar.

Tai Ingole, Student at Savitribai Phule Pune University,Department of Computer Engineering,Shri Chhatrapati Shivaji College Of Engineering Shrishivajinagar.

Pratiksha Surwase, Student at Savitribai Phule Pune University,Department of Computer Engineering,Shri Chhatrapati Shivaji College Of Engineering ,Shrishivajinagar.

Cryptography is technique of sending and receiving encrypted messages such way that decryption can perform by using mathematical algorithm or computations such that no one but only authorized receiver can decrypt the message and read the message. To overcome this new method introduced the visual cryptography scheme(VCS) as a simple and secure way to allow the secret sharing of images without any cryptographic computations.

C. Visual Cryptography

Visual cryptography is a cryptographic technique which allows visual information such as picture,text, private image etc. which to be secure is encrypted such a way that decryption can perform without using any mathematical computation. In visual secret sharing scheme image is broken up into n shares so that only someone with all of n shares could decrypt the image,while an n-1 shares not gain any information about original image. Decryption is perform by superimposing the shares.

II. EXISTING APPROACH

Existing approach used cryptography techniques which is process of converting information to unreadable format so that only authorized person with key can access that information. Now a day the field of communication becomes very advanced.It is become simple to decrypt cheaper text. So new scheme visual cryptography come in focus. In predefined visual cryptography scheme uses pixel expansion technique. So reconstructed image will be twice of its original width due to pixel expansion. Hence performance of system can degraded characteristics due to loss in clarity.

III. PROPOSED APPROACH

A. System Architecture:

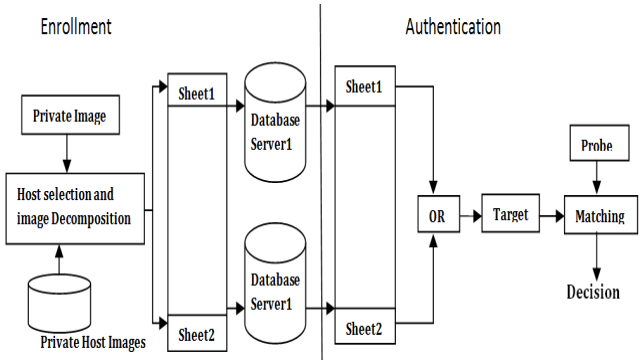

Fig: System Architecture

B. Modules

i)Enrollement Module:-

During the enrollment process images is make visually unrecognizable. Unauthorized users have not decrypt the private image to access the original image. The original image can be decomposed into sheet each one containing a specific number of pixels. The decomposed components are then transmitted and stored in two different database servers. Where XOR is Boolean operation Sh is an image as which appears as white noise k should less than or equals to noisy images. It is difficult or impossible to gain secret image T using individual sheet , encryption is perform very clearly or properly in such way that k or more out of n generated images must be necessary or required for reconstructing or decrypting original image T .

ii)Authentication Module

Sheets are superimposed in order to reconstruct the private image. An reverse pixel expansion process perform to get original target image.

iii)Visual Cryptography Scheme:

Naor & Shamir work on VCS. They introduced a[2] new technology that allows secret sharing of images in such way that only intended user i.e. user with specific key can decrypt or read the message or image without any cryptographic computation or mathematical Algorithm. VCS is decryption of encrypted information is carry out by using human visual system, is used for that k out of n VCS which is denoted (kn) VCS is used .For performing VCS we given a original image as T. Which is encrypted into a n images such that n is number of noisy images. The original image is encrypted such as

T=Sh1 XOR Sh2 ……XOR Shk

Each pixel P of the original image encrypted into two subpixel called as shares .Choice for encrypting the pixel into subpixel is randomly determine .

There are two choices are available for each pixel P of original image .Single share can not give any information about the original pixel.When two share are superimposed then and then only value of original pixel is gain Or obtain.

We get two black subpixel for black pixel P in original image and we get one black subpixel and one white subpixel for white pixel P in original image.Due to these subpixel encryption reconstructed image will be twice of width of original private image.

VCS used for providing privacy to biometric data such as iris code and fingerprint. Nakajima & Yamaguchi [3] introduced two out of two extended VCS for natural image such as face images. They introduced new technology for encrypting natural images in host images such that no one can guess there is existence of secret information. In VCS we divide image into shares by pixel expansion so that inspector may be guess there is any screcet information ,so we use GEVCS for securing face images.

III) GRAY-LEVEL EXTENDED

A. Visual Cryptography Scheme (GEVCS):-

In VCS secret image is divided into n sheet images which cannot give any idea about original image, each of these sheet contains random set of pixel. Ateniese works on VCS and introduced new method GEVCS .In this method gray-level image converted into meaningful binary image known as Half-toning and newly form image is called half-toned image. Then perform Boolean operation on Half-toned pixel of two host images. Some important terms in GEVCS are as follows:

B. Digital Half-toning:

Digital Half-toning is also called pixel expansion.

It is technique of converting digital grayscale image into array of binary values.In printing process this values are represented by dots.Error diffusion is one type of half-toning technique in which if quantization error occur during processing then it distributed to nearest pixel which still not processed .During pixel exapanssion process at pixel level any continuous set of pixel expanded to matrix of black and White subpixel .

i. Encryption :

Three half-toned images can be encrypted on pixel by pixel basis. Number of white subpixel denoted by transparency triplet. Required transparency of target pixel can be manage by arrangingthe subpixel in both shares. Pixel transparency triplet denoted by (t1t2tT).where

t1,t2and tT are transparencies of subpixel for share1,share2 and target subpixel respectively.In some cases required transparency for pixel in target cannot obtain. Therefore for determining possibilities of achieving the target transparency by re-arrangement of white subpixel in the shares.Target transparency must be in specific range.

IV. SECURING PRIVATE FACE IMAGES

Consider P is public database containing set of candidate image(H1,H2-------Hn).This host images used to hide a private face image O. First step towards the encryption is select host image Hi and Hj such as i not equal to j. From set of candidate host image database P containing host images there is variation in geometry and texture of private image T and image in public dataset .Selection of host image from database for hiding private image should be carried out properly .Selection of host image impact on the target image and generated sheet. So to reduced effect we should select host image properly for encryption of private image. For proper selectionof a host images active appearance model is used.

V. ACTIVE APPEARANCE MODEL

AAM select host images that most similar with private image by using geometry and appearance characteristics in AAM face and texture properties are utilized to verify similarities between private image and host image[4] .Some steps for building AAM :

A. Annotation of the training set:

For each image in public dataset there face features annotated manually by using landmark of predefined shape.

B. Create Shape model:

Due to given transformation shape of image affected.This effect is removed by using shape alignment process.Principal component analysis used to build linear model of shape differences between images in training set.

C. Create Texture Model :

Using annotated landmark of predefined shape.All images in public dataset wrapped to there mean shape. Then each pixel is wrap image sufficient to create texture vector. Lighting Effect on texture vector reduces using photometric normalization.
VCS, so it is impossible 4)Build Combined AAM:
Shape and texture model are compare with each other.PCA used to construct combined model from shape model and texture model.
That combined model consist of combined parameter C.

D. Annotating an image

Error between the private image and synthesized image is minimized using combined parameterss.

E. Host selection

For selecting host images compactible with private image cost of alignment of private image with candidate host image in database take into consideration these cost is known as transformation cost(Tc).Along transformation cost appearance cost(Ac) take into consideration these appearance cost related with texture.

F)Image Registration and Cropping

Two selected host image and private image align using global affine transformation component. Align host image and private image cropped to capture only facial feature which has been located by AAM.

E) Secrete Encryption And Registration

GEVCS used to encrypt secret image into two selected host image. After encrypting two sheets are form s1 and s2.then two sheets s1 and s2 are superimpose to get original image. By using reverse pixel Expansion it is possible to retain original image of original size.

VI. CONCLUSION

The contribution of this paper includes a methodology to protect the privacy of a face data-base by decomposing an input private face image into two independent sheet images such that the private face image can be reconstructed only when both sheets are available at the same time. The proposed method selects the host images that are most likely to be compatible with the secret image based on geometry and appearance. Encrypt the private image in the selected host images. It is observed that the reconstructed images are similar to the original private image.In this paper, we give the biometric privacy using visual cryptography. We provide the security to the biometricdata. In this the templates are divided into two imagesusing to recover the original image without accessing two the shares. For superimposing two images XOR operation use .

REFERENCES

[1] Arun Ross, Senior Member, IEEE ”Visual Cryptography for Biometric Privacy “,IEEE Trans.March 2013.

[2] M. Naor and A. Shamir,Visual cryptography.