RESEARCH ARTICLE OPEN ACCESS

Visual Cryptography for Image Privacy

Miss. Shubhangi Rajanwar [1], Mr. Shirish Kumbar [2], Mr. Akshay Jadhav [3]
Prof. Saba Siraj [4]
Student [1], [2] & [3], Assistant Professor [4]
Department of Computer Science and Engineering
IOKCOE Pune
Maharashtra - India

ABSTRACT

In information technology, biometrics refers to technologies that measure and analyze human body characteristics, such as DNA, fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for authentication purposes. “Biometric” is taken from the two words ‘bios’ and the 'metricos' which belong to the Greek language and it stands for "life measure". The biometrics is user friendly. So to work with the biometric data we would have to collect some raw data in order to process it and then that raw data is compared with the data stored in the databases. While doing so there is a strong possibility of facing attacks on the system, that is why we have to give more privacy to our Biometrics data. Biometrics systems are having physical and behavioral features like, face, fingerprints etc. So the purpose is to protect the biometric data from the attackers for that we are using visual cryptography. Cryptography is the secret communication of the images with the authorized persons.

Keywords:-Simple Block Replacement (SBR), Extended Visual Cryptography (EVS), Floyd Steinberg Error Diffusion, Gray Scaling, Rescaling, Pattern Matching.

I. INTRODUCTION

1.1 About The Project

In current times identity of a person is what matters the most, so in order to preserve it we are proposing a concept "Visual Cryptography for Biometric Analysis' under which we are providing security to the images. We are bringing this concept forward in order to provide more security to images with critical importance.

1.2 Purpose of the Project

Whenever we are dealing with our data (images) in terms of sending and receiving, there is a strong possibility of getting attacked midway. In order to provide more secure way of transmission and

handling we will encrypt our data (images) and then only send it to the intended receiver, at the other end the recipient when gets this data will decrypt it with the same module/process used for encryption and get the final result. Visual cryptography traditionally comes with a guarantee of security by means of defining perfect secrecy. Usually, a set of forbidden players is not allowed to learn any information about the (one) secret image even under the possibility of collusion. In our scheme, participants share different secrets with different people, thus we need to take this into account when defining security.

1.3 Domain Of The Project

1.3.1 Visual Cryptography

Visual cryptography is a phenomenon under which images are used and distributed as shares such that, when the shares are superimposed, a hidden secret image is revealed. In extended visual cryptography (EVC), the share images are constructed to contain meaningful cover images, thereby providing opportunities for integrating visual cryptography and biometric security techniques. We use the concept of Visual Cryptography in order to provide security for the images. We use this concept in such a way that the required (secret) image is separated in two parts and those two images are saved on the server geographically apart.

II. EXISTING SYSTEM

In the existing system, the VCS is a cryptographic technique that allows for the encryption of visual information such that decryption can be performed using the human visual system. Using this technique the biometric data is captured from the authorized user. This original image is divided in two cover images. Each cover image is stored in two different databases. When both images are simultaneously available then only we can get the original image. The individual share does not reveal any information about the original image. This technique is also used for iris codes. So the visual cryptography scheme is more secure for biometric template security. But it requires more space for storing sheet because of pixel expansion. So the size of the original image is becomes larger instead of original size this is the disadvantage of the existing system and we are countering this flaw in our project.

2.1 Drawback

The main drawback in VCS done so far is such that the size of the secret image happened to be much larger than its original dimensions (pixel expansion). The output image is hat we supposed to get after decryption, that image was increased in dimensions. We are countering this flaw in our proposed system.

III. PROPOSED SYSTEM

In Visual Cryptography, there are some algorithms for encryption and decryption of images. In this Project we are using one secret image and two cover images, and these images are overlapped with each other so that the secret image is secured in the two cover images. So if these two cover images are simultaneously available then only we can access the secret image. The single share can't give any information of the secret image. We are using the encryption process including "Floyd Steinberg Error Diffusion" algorithm for Half toning an input image and convert into Gray Scale image in the range 0-255. We are also using Simple Block Replacement(SBR) algorithm for storing the images pixels in the databases with the proper order where the secret image is secured with cover images and the decryption process is an OR operation. So when the pixel values are at the defined positions that are read from those two shares and then the minimum of the two is selected as the pixel value of the secret image. First we have to register into the system, for registrations we have to fill the username, email-id, and password and upload secret image and two cover images. After that when we login into the system then we have to enter the password and the secret image, if the secret image which is entered by the user is matched with the original secret image then we consider that he or she is the authorized person. If the pattern matching percentile is less than 98% then we consider that the user is unauthorized. We are using the concept of rescaling, gray scaling, Half toning, and pattern matching.

3.1 Extensive Technical Research

3.1.1 Visual Cryptography Scheme (VCS)

In the existing system of the visual cryptography, all of the images (secret and cover) must be of the same size and all the images must be black and white images or gray scale images. In our proposed system we are using rescaling module such that when we upload the secret and cover images irrespective of their sizes, the rescaling module rescales them to a fixed size. So in our proposed system this bug is countered. In the VCS, it allows one to encode the secret image into different sheet images, which is having no information about the secret image. The sheets are the random sets of the pixels of image; they may get the curiosity of an interceptor by giving the existence of the secret image.

3.1.2 Rescaling Module

In earlier times it used to happen that whenever we upload images, the secret image turns out to be of larger size in terms of pixel resolution. To counter this problem rescaling algorithm was introduced which functions in such a way that when we upload images irrespective of their pixel size variances, then we can restrict the size of the images to a fixed size and reveals the output image of the same size. Visual Cryptography works only on the black and white images and images of the fix size. If the uploaded images of different sizes then visual cryptography would not work. So we are resizing those images into a fix size by using rescaling module.

Rescaling Steps:

1. Read the original image.
2. Define the new height and width of rescaled image.
3. Create Graphics2D object and give the rescale image.
4. Draw the original image on the rescaled image.
5. Return the rescaled image.

3.1.3 Gray Scaling Algorithm

Visual Cryptography does not work on the colored images, in accordance to that we are here converting those images into grayscale image pattern such that later it will appear to be a black and white image. We can upload the images irrespective of their color and size, because later they will be rescaled and converted into a black and white image. We can extract the RGB features out of an pixel by using the following formula.

"Gray scale = r*0.21+g*0.71+b*0.07"

Grayscale image conversion:

1. Read the original image.

2. Define a new blank image of same height and width of original image. The blank image will be our gray image.
3. for i=0 and i<original image, repeat step 5,6,7.
4. for j=0 and j<original image height, repeat step 5,6,7.
5. Read the red, green and blue component individually for pixel at position (i,j).
6. grey = 0.21*red+2.71*green+0.07*blue.
7. Set grey at position (i,j) in grey image.
8. Return Grey image.

3.1.4 Floyd–Steinberg Error Diffusion Algorithm

In this technique, Digital Halftoning Method is used. There are some printer devices that do not contain so many shades of the gray color. If minimum shades are available then it will print only that number of minimum shades otherwise it will not print. So by using printer palate we can define our own values for the palate. e.g. if we have defined palate values as (0 70 120 180 255) then every pixel which is having values nearer to the palate values then that palate value is assigned to that pixel. This is the new value of that pixel. e.g. if the pixel value is 60 then 70 is nearest value for the pixel then 70 is assigned to that pixel instead of 60. The initial value of that pixel is 60 and extra is 10 (70-60), thesis occurring as a quantization error. So we have to remove this error by using error diffusion method. Error diffusions a type of halftoning in which the quantization residual is distributed to neighboring pixels that have not yet been processed. Its main use is to convert a multi-level image into a binary image, though it has other applications. Unlike many other halftoning methods, error diffusion is classified as an area operation, because what the algorithm does at one location influences what happens at other locations. This means buffering is required, and complicates parallel processing. Point operations, such as ordered dither, do not have these complications. Error diffusion has the tendency to enhance edges in an image. This can make text in images more readable than in other halftoning techniques.

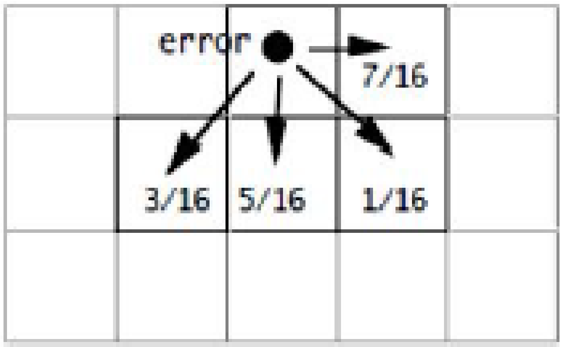

Fig 3.1.4: Error Diffusion.

In the above diagram the error is diffuse with nearest four pixels. That error is nothing but the quantization error which is diffused with the four neighboring pixels as shown in the above diagram

Algorithm: Floyd and Steinberg error diffusion halftoning

```
for each y from top to bottom
  for each x from left to right
        old pixel := pixel [x][y]
        new pixel := find_closest_palette_color(oldpixel)
        pixel[x][y] := new pixel
        quant_error := oldpixel - newpixel
        pixel[x+1][y] := pixel[x+1][y] + quant_error * 7/16
        pixel[x-1][y+1] := pixel[x-1][y+1] + quant_error * 3/16
        pixel[x][y+1] := pixel[x][y+1] + quant_error * 5/16
        pixel[x+1][y+1] := pixel[x+1][y+1] + quant_error * 1/16
   end for
end for
```

3.1.5 Simple Block Replacement (SBR) Algorithm

After creating a halftone image, in order to preserve the image size when applying visual cryptography and extended visual cryptography, simple methods can be applied. We refer to this basic approach as simple block replacement (SBR). The SBR scheme considers groups of four pixels from the halftone secret image in one 2 * 2 block, referred as a secret block, and generates the shares block by block (rather than pixel by pixel). As each secret block with four pixels encodes into two secret shares each containing four pixels, the size of the reconstructed image is the same as the original secret image after stacking the two shares together. In this technique, all the secret blocks in an image need to be processed before visual cryptography encoding and each secret block is replaced by the corresponding predetermined candidate, which is a block with 4 white pixels (a white block) or a block with 4 black pixels (a black block). The block replacement process in the SBR pre-processing scheme is based on a number of black and white pixels in each secret block. If the number of black pixels in a secret block is larger than or equal to 2, the secret block converts to a black block. If the number of black pixels in a secret block is less than or equal to 1, it is converted to a white block. This step produces a new secret image which contains only white and black blocks. The image obtained from this step is referred to as a processed secret image. The processed image is now ready to be used as a secret image in visual cryptography schemes such as traditional VC or EVC. The SBR approach is straightforward and is very effective for unprocessed binary secret images which have large numbers of all white and all black blocks. However, for halftone images, with high variability in the distribution of black and white pixels within each secret block, the resulting processed secret image is generally poor, being darker than the original image, with poor contrast, causing the loss of many fine details in the images.

3.1.6 Pattern Match Algorithm

Pattern Matching is the act of checking a given sequence of tokens for the presence of the constituents of some patterns. When we access the secrete image then that image is compared with the image stored in the database. There are two things that such as either we can match black colors or we can match via white colors. Here we are using white color matching because it is more effective and secure for matching the images.

3.2 ADVANTAGE

1. No pixel expansion the size of the secret image is as it is.

2. High Level Security for the biometric privacy.

3. Prevent Attacks of biometric images.

4. Secure Databases.

3.3 SYSTEM ARCHITECTURE

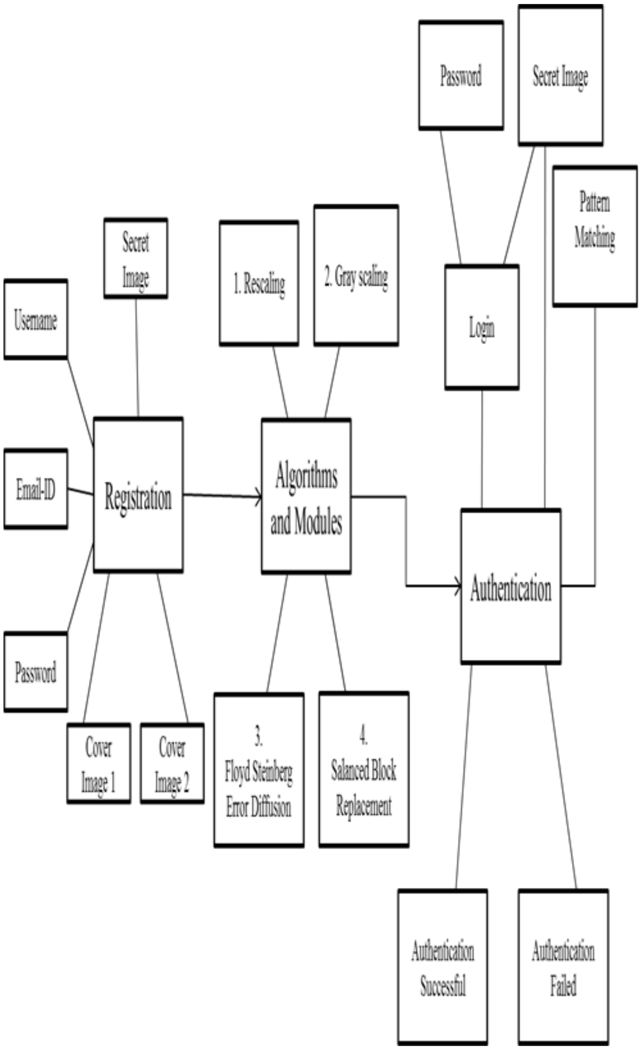

Fig.3.3: System Architecture for Proposed System.

In the above system architecture, It shows the overall structure of the VC i.e. Visual cryptography system. First we have to register into the system by using the email_id, username, password, secret image, cover image one and cover image two. After the registration the VC application performs the modules and algorithms on the images which are Rescaling, Gray scaling, Floyd Steinberg Error Diffusion. After this we have to login into the system then we have to enter the password instead of using username and we are using secret image as the password that we have to enter in the login, Then the entered image is compared with the secret image which is stored into the database. if the entered image is matched with the database then the authentication is successful otherwise there is not the authorized person. There are two ways to check the matched pixels of the image is by using the black pixels matched values and by using the white pixels matched values of the images stored in the database. We are using so the white pixels of the image for the pattern matching. Normally the images required less no of the white pixels so if the white pixel matched is about 25% or greater than the 25% then the image is considered as the secret image or if the match is less than the 25% then the image is not secret image.

3.4 Mathematical Model

The following table shows the steps of execution of mathematical model. Which includes the the mathematical statements for the modules and algorithms which are used in the Visual Cryptography For Image Privacy. It is having the sets and functions which are used in the algorithms and modules. So that the table shows the Mathematical Terms used for the project.

Table 3.4: Mathematical Model

Sr.No	Description	Observations/Remark
1	Let S be the System S={S1, S2, S3} Where, S1- module that authenticates S2- the module that registers user S3- the module that decrypts images	S identifies system set
2	S1={I,P,O,In,C,Sc,F} I=Input P={P1,P2,P3} O=Output In=Initial Condition as login C=Constraints Sc=success F=failure Where, P1- functions of uploading image P1={A1,A2,A3} A1- uploadImage(image,password) A2- grayScaleProcess() A3– halftoneProcess() P2- DBMS that handles the query P2={B1,B2,B3} B1- receiveImageQuery() B2- processImageQuery() B3- returnResult() P3- Functions for pattern matching P3={C1,C2} C1- overlap(image1,mage2) C2- match(image,overlappedImage)	The module that authenticates. Input: Password, Secret image. Output: Image. Constraint: We have to give the password and secret image.

3	S2={ I,P,O,In,C,Sc,F}
	Where,
	I=Input
	P=Process
	P={P1,P2,E}
	O=Output
		The module that registers users and starts the encryption process.
		Input: Image.
		Output: Image.
		Constraints:
		1. The uploaded images size is less than or equals

	In=Initial Condition as registration C=Constraints Sc=success F=failure Where, P1- functions of uploading image P1{A1,A2,A3} A1- uploadImage(image,password) A2- grayScaleProcess() A3– halftoneProcess() P2- DBMS that handles the query P2={B1,B2,B3} B1- receiveImageQuery() B2- processImageQuery() B3- returnResult() E- Functions for evcs encryption E={E1,E2} E1- evcs(image1,mage2,image3) E2- save (image,overlappedImage)	to the defined size. 2. We have to Upload all of the three images i.e. Secret image, Cover image1, Cover Image2. 3. We have to fill all of the required information i.e. Email_id, Username, Password, Images.

4	S3={I,P,O,C,Sc,F}
	Where
	I=Input as image
	P=Process
	O=Output
	C=Constraints
	Sc=Success
	F=Failure
	P={D1,D2}
	D1= upload(image1,image2)
	D2= decrypt(image1,image2)
		The module that decrypts.
		Input: Password, Secret image.
		Output: Image.
		Constraint:
		We have to give the password and secret image.

3.5 Graph

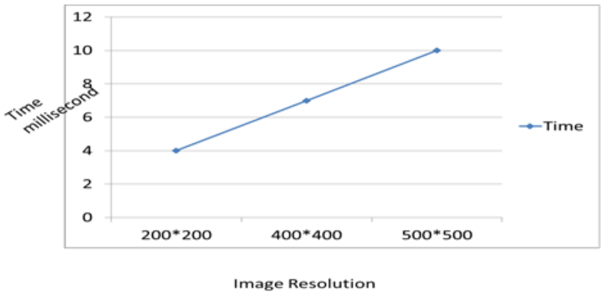

Fig 3.5.1: Graph for Time Efficiency of Existing System

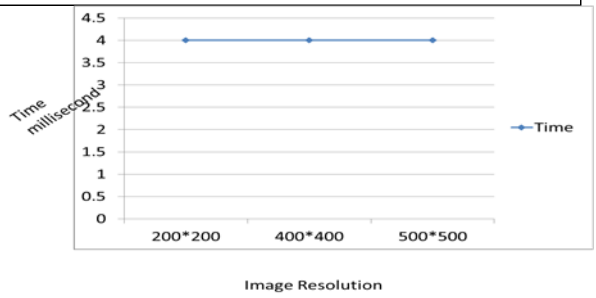

Fig 3.5.2: Graph for Time Efficiency of Proposed System

IV. CONCLUSION

Thus we have studied about to protect the image databases by decomposing an input private image into two independent sheets of the images such that the secret image can be reconstructed only when both the 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. And increasing the pixel expansion factor can lead to an increase in the storage requirements for the sheets. So in the 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 the random noisy images. Thus, more work is necessary to handle this problem.

V. FUTURE ENHANCEMENT

In the future instead of using raw image) we can use web cam. This can also be useful for all of the security related institutions like offices, military, confidential laboratories etc. It can work for the multiple system and multiple cover images, it can also work with the multiple databases for more security.

ACKNOWLEDGEMENT

We thank to Prof. Saba Siraj (Assistant Professor) for her useful guidance.

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, DilipkumarKotthapalli, "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.

[5] Arun Ross and Asem A. Othman, "Visual Cryptography for Face Privacy", Proc. of SPIE Conference on Biometric Technology for Human Identification VII, (Orlando, USA), April 2010.

[6] G. I. Davida, Y. Frankel, and B. J. Matt, "On enabling secure applications through off-line biometric identification," in *Proc. IEEE Symp.Security and Privacy*, 1998, pp. 148–157.

[7] Y. Feng, P. Yuen, and A. Jain, "A hybrid approach for face template protection," in *Proc. SPIE Conf. Biometric Technology for Human Identification*, Orlando, FL, 2008, vol. 6944.

[8] D. Bitouk, N. Kumar, S. Dhillon, P. Belhumeur, and S. K. Nayar, "Face swapping: Automatically replacing faces in photographs", *ACMTrans.Graph.*, vol. 27, pp. 1–8, 2008.

[9] B. Thuraisingham and W. Ford, "Security constraint processing in a multilevel secure distributed database management system", *IEEETrans. Knowl. Data Eng.*, vol. 7, pp. 274–293, Apr. 1995.

[10] N. Ratha, J. Connell, and R. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Syst. J.*, vol. 40,pp. 614–634, 2001.

[11] D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. Secaucus, NJ: Springer-Verlag New York, Inc.,2003.

[12] S. Prabhakar, S. Pankanti, and A. Jain, "Biometric recognition: Security and privacy concerns," *IEEE Security Privacy*, vol. 1, pp. 33–42, Mar./Apr. 2003.

[13] Souvik Roy and P. Venkateswaran, "Online Payment System using Steganography and Visual Cryptography", 2014 IEEE Students' Conference on Electrical, Electronics and Computer Science 978-1-4799-2526-1/14/$31.00 ©2014 IEEE.

[14] Prateek Kumar1, Suneeta Agarwal2, and Shivendra Shivani3 *1, 2, 3MNNIT Allahabad, Uttar Pradesh,* "Halftone Visual Cryptography with Pixel Expansion through Error Diffusion", International Journal of Information & Computation Technology. ISSN 0974-2239 Volume 4, Number 14 (2014), pp. 1419-1427 © International Research Publications House http://www. irphouse.com.

[15] AnandhiandS.Satthiyaraj," Embedded Visual Cryptography Schemes for Secret Images ", IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.12, December 2012 153 Manuscript received December 5, 2012 Manuscript revised December 20, 2012.

Author Profile

Miss. Shubhangi S. Rajanwar born on July 8, 1994 is pursuing BE Computer Engineering, from Savitribai Phule Pune University, Institute of Knowledge College of Engineering Pune, Maharashtra, India.

Mr. Shirish S. Kumbar born on July 8,1993 is pursuing BE Computer Engineering, from Savitribai Phule Pune University, Institute of Knowledge College of Engineering, Pune, Maharashtra, India.

Mr.Akshay A. Jadhav born on February 5, 1994 is pursuing BE Computer Engineering from Savitribai Phule Pune University, Institute of Knowledge College of Engineering, Pune, Maharashtra, India.