A PROPOSED SYSTEM ON EXTENDED VISUAL CRYPTOGRAPHY SCHEME FOR FACE PRIVACY

Swapnil Choudhary[1], Sagar Toke[2], Amit Bachal[3],
Piyush Chavare[4], Prof. Pallavi Patil[5]

[1, 2, 3, 4, 5]Department of Computer Engineering, JSPM Narhe, University of Pune, Maharashtra, (India)

ABSTRACT

The automobile engine connecting rod is a high volume production vital element. Every vehicle that uses an internal combustion engine requires at least one connecting rod .From the viewpoint of functionality, connects the rods must have the maximum possible rigidity at the less weight. The major stress induced in the connecting rod is a combination of axial and bending stress in process. The axial stresses are caused due to cylinder gas stress and the inertia force arising in account is due to reciprocal action (both tensile as well as compressed), where as bowing stresses are occurred due to the diffusive effects. The result of which is, the maximal stresses are developed at the fillet section of the big and the small end.

I. INTRODUCTION

Biometircs is the science of establishing the identity of an individual based on physical or behavioural traits such as face, fingerprints, iris, etc. The working of biometric authentication system acquires raw biometric data from a subject, extracting a feature set from the data, and comparing the feature set against the templates stored in a database in order to identify the subject or to verify a claimed identity. At the same time there is a possible to intruder can access the database which stored the biometric data. So the security and privacy of biometric system is a major concern due to their issues like fake biometric, override matcher and etc. The biometric data classified as physiological or behavioural. Physiological biometrics based on the physical part of the body such as fingerprint, iris, eye retina, face, palm, hand. Behavioural type is based the behaviour of human such as voice, signature and keystroke. Cryptography is the art of sending and receiving encrypted messages that can be decrypted only by the sender or the receiver. Encryption and decryption are accomplished by using mathematical algorithms in such a way that no one but the intended recipient can decrypt and read the message. Visual cryptography is introduced by Noar and Shamir. It is another form of cryptography in which secret communication is done in the form of images. This can be used to protect the biometric templates in which the decryption doesn't require any complex computations; it is done by human visual system. Using this visual cryptography the biometric data capture from the authorized user. These original images are divided into two shares .Each share stored in two different databases. When both images are simultaneously available then only we can get the original image. The individual shares do not reveal any information about the original image.

II. PROBLEM RELATED WORKDONE

2.1 Visual Cryptography Scheme (VCS)

One of the best known techniques to protect data such as biometric Templates is cryptography. It is the art of sending and receiving encrypted messages that can be decrypted only by the sender or the receiver. Encryption and decryption are accomplished by using mathematical algorithms in such a way that no one but the intended recipient can decrypt and read the message. Naor and Shamir introduced the visual cryptography scheme (VCS) as a simple and secure way to allow the secret sharing of images without any cryptographic computations. 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 visual cryptography the biometric data capture from the authorized user. These original images are divided into two shares .Each share stored in two different or same databases. When both images are simultaneously available then only we can get the original image. The individual shares do 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 sheets due because of pixel expansion.VCS allows one to encode a secret image into sheet images, each revealing no information about the original. Since these sheets appear as a random set of pixels, they may pique the curiosity of an interceptor by suggesting the existence of a secret image. To mitigate this concern Ateniese introduced new framework known as the extended VCS.

2.2 Digital Halftoning

Digital halftoning is a technique for transforming a digital gray-scale image to an array of binary values represented as dots in the printing process. In this section, we consider the application of visual cryptography to grayscale images by first converting the images to a binary image using a halftoning 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. Halftoning is a method for creating the illusion of continuous tone output with a binary device. Effective digital halftoning can substantially improve the quality of rendered images at minimal cost. Following are the methods of Digital half toning.

1] Thresholding

2] Constant Threshold

3] The Minimum Squared Error Solution

4] Ordered Dither

III. SYSTEM ARCHITECTURE

Following diagram shows the proposed system architecture. We are going to implement following module shown in diagram in Java language.

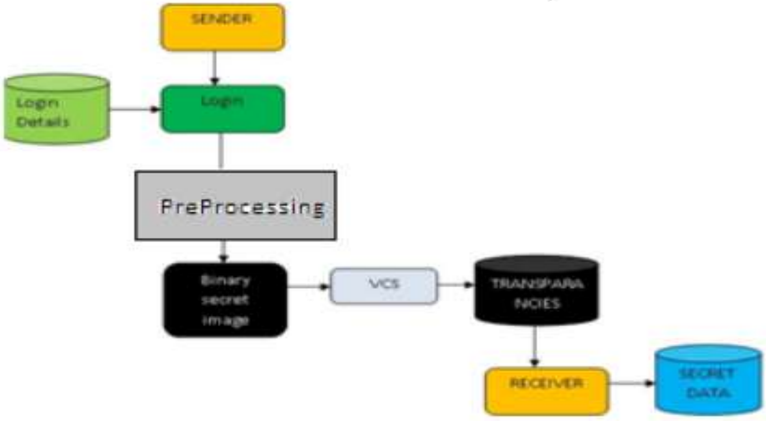


Fig.1. System Architecture

IV. METHODOLOGIES USED

4.1 Preprocessing Technique

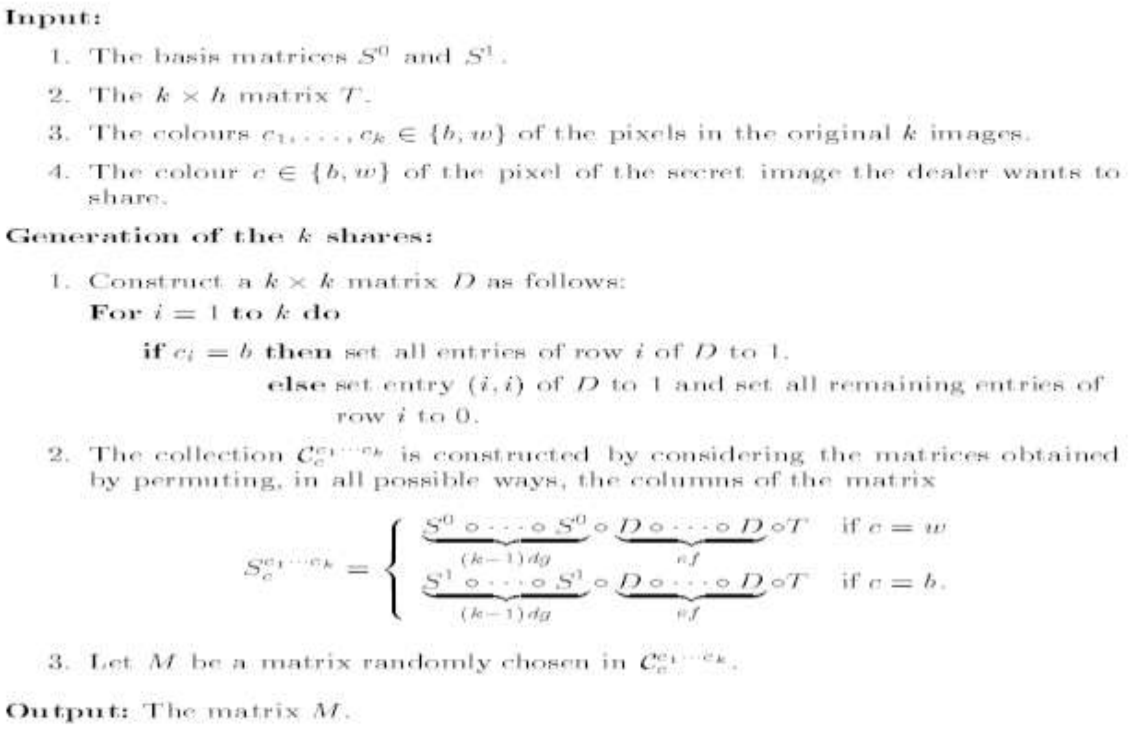
Floyd–Steinberg dithering is an image dithering algorithm given by Robert W. Floyd and Louis Steinberg. It is commonly used by image manipulation software, for example when an image is converted into GIF format that is restricted to a maximum of 256 colors.

The pseudo code for Floyd –Steinberg dithering algorithm is as follows-

```
for each y from top to bottom
  for each x from left to right
    oldpixel  := pixel[x][y]
    newpixel  := find_closest_palette_color(oldpixel)
    pixel[x][y]  := newpixel
    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
```

4.2 Encryption Method (Construction of Matrix)

The method explained in fig.2 is used for proposed extended visual cryptography system. The method is called as (k, k)-threshold EVCS.



Input:

1. The basis matrices S^0 and S^1.
2. The $k \times h$ matrix T.
3. The colours $c_1, \ldots, c_k \in \{b, w\}$ of the pixels in the original k images.
4. The colour $c \in \{b, w\}$ of the pixel of the secret image the dealer wants to share.

Generation of the k shares:

```
1. Construct a $k \times k$ matrix $D$ as follows:
   For $i = 1$ to $k$ do
       if $c_i = b$ then set all entries of row $i$ of $D$ to 1.
              else set entry $(i, i)$ of $D$ to 1 and set all remaining entries of
                  row $i$ to 0.
2. The collection $\mathcal{C}_c^{c_1 \cdots c_k}$ is constructed by considering the matrices obtained
   by permuting, in all possible ways, the columns of the matrix
```

$$S_c^{c_1 \cdots c_k} = \begin{cases} \underbrace{S^0 \circ \cdots \circ S^0}_{(k-1)dg} \circ \underbrace{D \circ \cdots \circ D}_{ef} \circ T & \text{if } c = w \\ \underbrace{S^1 \circ \cdots \circ S^1}_{(k-1)dg} \circ \underbrace{D \circ \cdots \circ D}_{ef} \circ T & \text{if } c = b. \end{cases}$$

3. Let M be a matrix randomly chosen in $\mathcal{C}_c^{c_1 \cdots c_k}$.

Output: The matrix M.

Fig.2 (k, k)-threshold EVCS Method

4.3 Decryption Method

Following is the pseudo code for decryption technique-

```
Read n share images.
for each y from top to bottom
    for each x from left to right
        $n_i$ = pixel[x][y];
secret[x][y] = min ($n_i$ pixel[x][y])
```

4.4 Face Detection Using Haar Cascades

In the proposed system, an additional module has been added for detecting faces. Face detection is carried out by using Haar Feature-based Cascade Classifiers. Haar feature-based cascade classifiers is an effective object detection method proposed by Paul Viola and Michael Jones [16]. It is a machine learning based approach where a cascade function is trained from a lot of positive and negative images. It is then used to detect objects in other images.

Here, in our proposed system we are using this method for face detection. Initially, the algorithm needs a lot of positive images (images of faces) and negative images (images without faces) to train the classifier. Then features are extracted from it. For this, haar features shown in fig.3 are used. These features are like convolutional kernel. Each feature is a single value obtained by subtracting sum of pixels under white rectangle from sum of pixels under black rectangle. Plenty of features are calculated by considering all possible sizes and locations of each kernel.

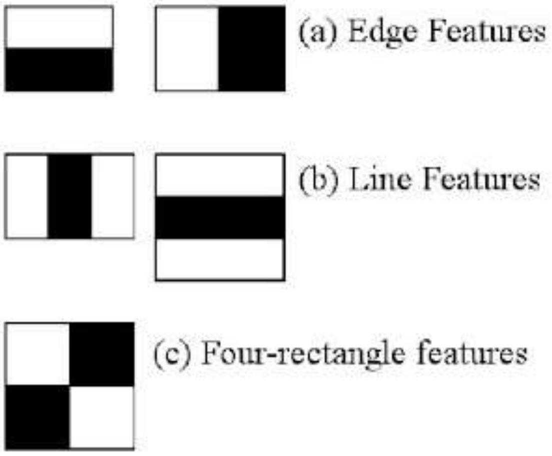


Fig.3 Haar Features

In an image, most of the image region is non-face region. So it is a better idea to have a simple method to check if a window is not a face region. If it is not a face region, then it can be discarded in a single shot. There is no need to process it again. Instead, the focus can be kept on the region where there can be a face. By following this way, more time can be spent to check a possible face region. The above discussed method is used in the concept of Cascade of Classifiers. Instead of applying all plenty of features on a window, group the features into different stages of classifiers and apply one-by-one. If a window fails the first stage, discard it. There is no need to consider remaining features on it. If it passes, apply the second stage of features and continue the process. The window which passes all stages is a face region. In this way, face detection is carried using Haar cascades.

V. CONCLUSION

In this paper, a scheme for Extended Visual Cryptography has been proposed for maintaining the perfect security of original image. By using an intelligent pre-processing of halftone images based on the characteristics of the original secret image, a good quality images in the shares and the recovered image are produced. In this paper, Otshu method is proposed to perform binarization and clustering-based image thresholding. In this paper, Otshu method is implemented in and hence all security features of the object oriented Java language will be seen in the proposed system.

REFERENCES

[1] N. Askari, H.M. Heys, and C.R. Moloney, "An Extended Visual Cryptography Scheme Without Pixel Expansion For Halftone Images", IEEE, 2013

[2] G. I. Davida, Y. Frankel, and B. J. Matt, "On enabling secure applications through off-line biometric identification," in Proc. IEEE, 1998.

[3] 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.

[4] D. Bitouk, N. Kumar, S. Dhillon, P. Belhumeur, and S. K. Nayar, "Face swapping: Automatically replacing faces in photographs," ACMTrans. Graph, 2008.

[5] B. Thuraisingham and W. Ford, "Security constraint processing in a multilevel secure distributed database management system," IEEE Trans. Knowl. Data Eng., Apr. 1995.

[6] N. Ratha, J. Connell, and R. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," IBM Syst. J., 2001.

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

[8] S. Prabhakar, S. Pankanti, and A. Jain, "Biometric recognition: Security and privacy concerns," IEEE Security Privacy, 2003.

[9] M. Naor and A. Shamir, "Visual cryptography", in EUROCRYPT '94 Proceedings, Lecture Notes in Computer Science, Springer-Verlag, 1995.

[10] A. Ross and A. A. Othman, "Visual Cryptography for Biometric Privacy", IEEE Transactions on Information Forensics and Security, 2011.

[11] G. Ateniese, C. Blundo, A. De Santis and D.R. Stinson, "Extended Capabilities for Visual Cryptography", Theoretical Computer Science, 2001.

[12] Z. Zhou, G.R. Arce, and G. Di Crescenzo, "Halftone Visual Cryptography", IEEE Transactions on Image Processing, 2006.

[13] M. Nakajima and Y. Yamaguchi, Extended Visual Cryptography for Natural Images, in Proceeedings of WSCG, pp. 303-310, 2002.

[14] C.L. Chou,"A Watermarking Technique Based on Nonexpansible Visual Cryptography", Thesis, Department of Information Management, National University, Taiwan, 2002.

[15] C.C. Wu and L.H. Chen, "A Study on Visual Cryptography", Thesis, Institute of Computer and Information.

[16] Paul Viola and Michael Jones ,"Rapid Object Detection using a Boosted Cascade of Simple Features", 2001.

AUTHOR PROFILE

	Prof. Pallavi Patil (*M.E. Comp) Department of Computer Engineering, JSPM Narhe, University of Pune, Maharashtra, India*
	Swapnil Choudhary (*B.E. Comp) Department of Computer Engineering, JSPM Narhe, University of Pune, Maharashtra, India.*
	Piyush Chavare (*B.E. Comp) Department of Computer Engineering, JSPM Narhe, University of Pune, Maharashtra, India*
	Amit Bachal (*B.E. Comp) Department of Computer Engineering, JSPM Narhe, University of Pune, Maharashtra, India*
	Sagar Toke (*B.E. Comp) Department of Computer Engineering, JSPM Narhe, University of Pune, Maharashtra, India*