Visual Cryptography in Biometrics Passport

Dhara Trivedi [1]
[1] Computer Science
Pacific Academy of Higher Education and Research University
Udaipur, Rajasthan, India
drtrivedi.it@gmail.com

Dr, Jigar Patel [2]
[2] Computer Science
Kalol Institute of Management
Kalol, Gujarat, India
drjigarvpatel@gmail.com

Abstract— Every human being is unique in their nature such as traits and physical symptoms so computer science is using the biometric for perfect identification within large database. Visual cryptography scheme is a cryptographic technique, which allows visual information e.g. printed text, handwritten notes, and picture to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. Biometric passport is a smart card technology product created by use of biometric data and computer chip for authenticate identification of citizen of particular country. Current passport has certain shortcoming. In this method it is proposed to convert scan images of retina, fingerprint and face in secret image and meaningful shares by use of visual cryptography. In this method with use of Visual Cryptography three biometrics i.e. retina image, fingerprint image and face image encrypted in two meaningful shares when these two share stacking on one another fingerprint image revealed and that can be verified with on the spot live fingerprint image for perfect identification accuracy.

Keywords- *Biometric, Biometric-passport, Visual Cryptography*

*****

I. INTRODUCTION

Government certifies the identity of citizen in Passport. As the anti social activity is become burning problem for the world in this millennium. Some governments have started to switch over on e-Passport and certain other countries including India are in process to issue e-Passport in near future. In e-Passport smart card technology with biometrics and digital signature is used. In this e-Passport human biometrics such as face image, fingerprint and Iris image utilize for identity so it is recognize as a biometric passport. The unique information of the person is store in a computer chip that is kept in passport with help of reader and the chip particular person can be identified in the safe manner. Current e-Passport shortcomings are Data may be migrated with advance technology, Obtain personal information by unethical hacking, Cloning and Cracking, Expensive for passport holder, Costly for the government.

With use of biological science and computer science identification of human by the traits has been used in emerging field of technology that is called biometric. Biometric is based on unique and sustainable physical characteristics face recognize, fingerprint, iris image, DNA, Palm print, retinal image, body odor etc. In these scheme main three biometric identifiers has been used as they are unique to individual and give more accurate in verification when used simultaneously. Face Recognize is verifying or identifying person from digital image. Fingerprint is an impression of human finger. It is most useful tool in investigation for perfect identification. Human retina is a natural pattern of blood vessels located at back portion of the eye. Each person retina is unique even identical twins have different pattern of retina. Retina remain unchanged from birth to death, so retina is a most precise and reliable biometric.

Visual cryptography is introduced first in 1994 by Naor and Shamir. Visual cryptography scheme is a cryptographic technique, which allows visual information (e.g. printed text, handwritten notes, and picture) to be encrypted in such a way the decryption become mechanical process that does not require computer. Naor and Shamir illustrated visual secret sharing scheme, where an image divide into n shares so that particular person stack all n shares could decrypt the image, while stacking time any n-1 shares could not reveal any information about original image. There are various measures on which performance of visual cryptography scheme depends, such as pixel expansion, contrast, security, accuracy, computational complexity, share generated is meaningful or meaningless, type of secret images (either binary or color) and number of secret images (either single or multiple) encrypted by the scheme. Visual cryptography scheme eliminates complex computation problem in decryption process and the secret images can be restored by stacking operation. This property makes visual cryptography especially useful for the low computation load requirement.

In the proposed method main weightage is on the security of the passport with the use of latest finding of biometrics and VC. This way we can reduce the cost of passport to the nations and the citizens. In the highly populated developing country like India, it is utmost required to the cut expenditure to issue more than 10 million passports per annum.

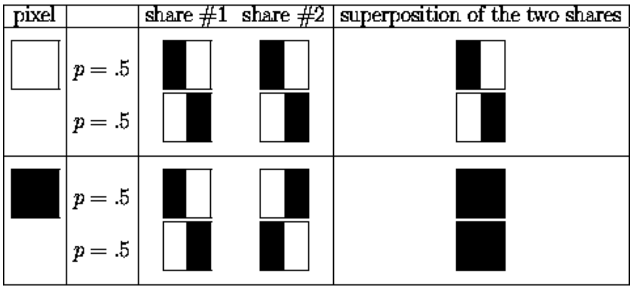
The paper is scheduled as under section II Related work, section III Methodology and Section IV Conclusion.

II. RELATED WORK

Naor and Shamir's [1] proposed encoding scheme to share a binary image into two shares Share1 and Share2. If pixel is white one of the above two rows of Table 1 is chosen to generate Share1 and Share2. Similarly If pixel is black one of the below two rows of Table 1 is chosen to generate Share1 and Share2. Here each share pixel p is encoded into two white and two black pixels each share alone gives no clue about the pixel p whether it is white or black. Secret image is shown only when both shares are superimposed.

The transparencies consist of randomly located white and black pixels. When stacking these transparencies together the secret message, e.g. an image or a text, is revealed. The decryption is executed by the human visual system and only the ownership of all transparencies can reveal the secret. Above figure illustrates the abstract work flow of encrypting and decrypting information by means of visual cryptography.

Table1. Naor and Shamir's scheme for encoding a binary pixel into two shares



pixel		share #1	share #2	superposition of the two shares
□	$p = .5$	■□	■□	■□
	$p = .5$	□■	□■	□■
■	$p = .5$	■□	□■	■■
	$p = .5$	□■	■□	■■

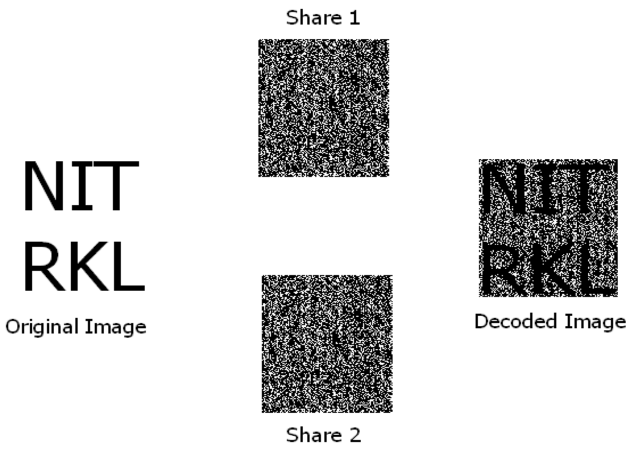


Fig.1: Visual cryptography

Visual cryptography is a perfectly secure encryption mechanism, and the decryption process is done by the human visual system. The cipher text is a printed page, and the key is a printed transparency of the same size. When the two are stacked and aligned together the plain text is revealed. Knowing just one of these two shares does not reveal any new information about the plaintext. This encryption scheme can be also considered as 2-out-of-2 secret sharing scheme (the two shares being the cipher text and the key), and it can be generalized to a k out of n secret sharing scheme. There has been considerable interest in visual cryptography, including suggestions, which improve the contrast of the resulting image [12, 6, 2, 4], or add color to the image [11, 13].

There have been many paper published related to visual cryptography. Many of them related to black and white visual cryptography and some color visual cryptography with different techniques.

In Zhou [3] method, Halftone visual cryptography is a kind of visual secret sharing scheme, which can decode a secret image by overlapping multiple binary share images. Visual cryptography secret sharing scheme can be used in the application with access control. By applying blue noise halftoning theory into the constructions mechanism of conventional visual cryptograph, visually pleasing halftone share caring significant data can be obtained. It can be used in a various visual secret sharing application such as watermarking, electronic cash, bank account operated by multiple users.

Threshold array are used to generate halftone share images from an input images. By using multiple threshold array in [16] halftoning method of VC, high speed processing with more extensibility can be achieved.

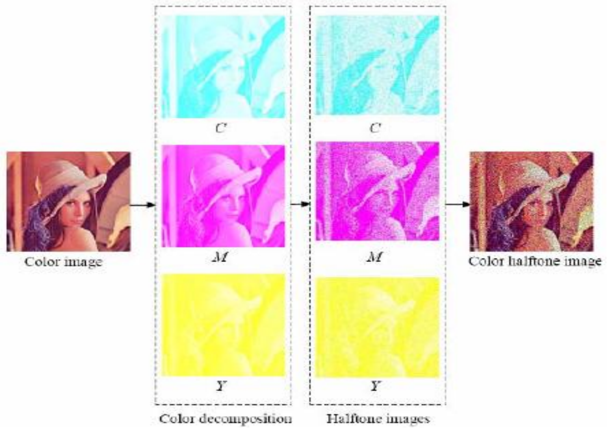


Fig.2: Color Decomposition and halftoning

In [5] use of three methods for Visual Cryptography. Color Visual Cryptography, the Halftone Technology and color decomposition see fig 2. He defines three different technique on based of their algorithms and experiment and got their method for color and black & white VC. They construct c-color (k,n) threshold scheme for any number of colors c and any number of k 2 ≤k ≤n.

This [7] method modification and extension of black and white VSS scheme. The colored VSS scheme using transparency as the shadow material which is easily recognize by human eye sight.

Superimposing many pixel of same color might result become more dark but [8] proposed method reconstruction secret pixel exact same color. They prove c color(n,n) threshold scheme are optimal with respect to pixel expansion.

This [10] method is very simple and efficient. This proposed method depend on two thing Error diffusion and VIP Synchronization, Its generate colorful meaningful share and high quality decrypted share. First they construct EVC scheme with VIP Synchronization and error diffusion for visual quality improvement. VIPs synchronization the position pixels that carry original image across the color channel so pixel value as same before and after encryption. And error diffusion is used to construct the share such that noise introduced by preset pixel are diffused away neighbors when encrypt.

Other proposed method generated meaningless shares so attacker can easily reveal secret image.

In [15] method they generated meaningful shares. First authors did color halftone transfer use of color decomposition and then extract pixel from color halftone image in fig 2. For they use two cover image and a secret image. They apply coding table on those images and create shares see in fig 3. For encoding procedure two coding table applied as a CCT for cover image coding table and SCT for secret coding table. SCT works in same as Hou's second method [5]. Whenever two share stack together secret Image revealed in decoding procedure see fig 4.

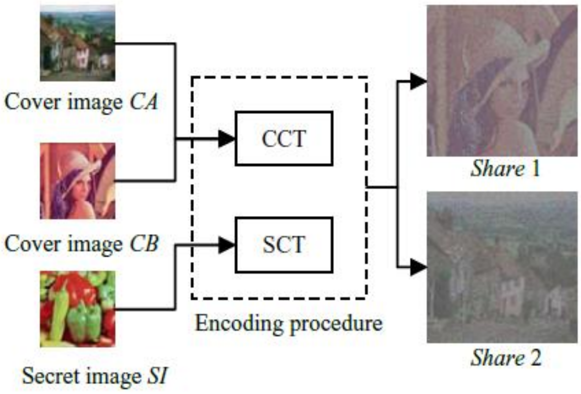


Fig.3: Encoding Procedure

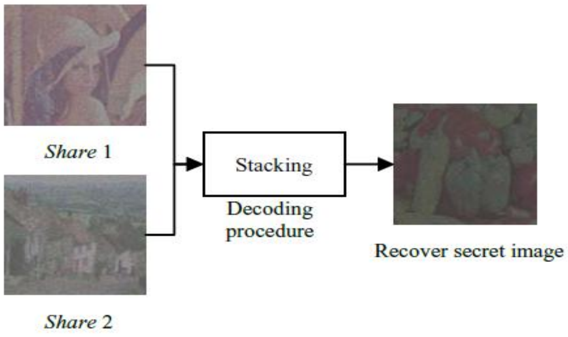


Fig.4: Decoding Procedure

They use color halftone transformation and pixel extraction to get clear image.

III Methodology

During the process of registration and issuing of passport along with identification documents persons unique biometrics that is retina, fingerprint and face image be obtain to create E-Passport after applying Visual Cryptography.

Three Unique biometrics, human face image, fingerprint and retina image can be successfully used for robust identification method. When we apply Visual Cryptography on the biometrics to obtain two meaningful shares, it becomes easy to store the shares in the database and passport.

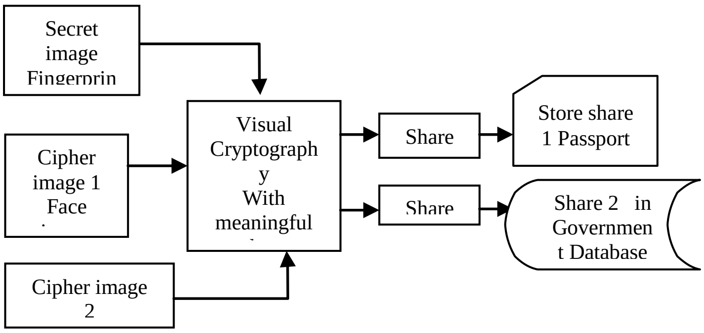


Fig.5: Encryption Process

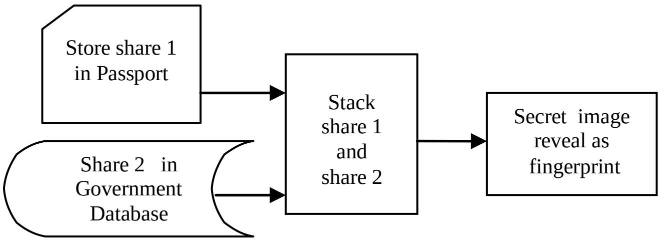

Store share 1 in Passport
Share 2 in Government Database
Stack share 1 and share 2
Secret image reveal as fingerprint

Fig.6: Decryption Process

In Encryption method of VC secret image as a fingerprint and cover images retina and face image. These cover images encrypted as two meaningful shares. From those shares, share 1 face image assign to passport as a user image and share 2 retina image save in government database for future verification (shown in fig 5).

At the point of authentication when share 1 and share 2 stacks then revealed fingerprint image (secret image) in decryption process (shown in fig 6).

Passport is a tool of identification for international use given by particular country. Passport is useful document for international mobility.

In this system citizen opens the website drafted for passport related work, sign up a new account on the site. This account can be any time login after sign up is completed with email, password and confirm password fields.

On the site after login user can get two options : Registration for passport and Application Status. User click on Registration link to open the Application form. Fill up the basic personal information such as Name, Birth date Address, Mobile, Education Qualification, Details of Identification etc in the form. When all required data furnished, after clicked on submit all details store in USER_DETAIL table and user get Registration No. After process period over when the person login the account and click on Application Status link, he can get interview Time, Date and Venue for further process to complete the formality the passport.

At the time of admin login four links: Request List, Verification, Passport Process and Identification. When admin clicks on Request List he will get all the request application with complete user details information with compile serially indicating time and date of registration. After authority clears the application one by one on merit, the short listed applicants will be allotted the date, time and venue for next round of passport process. On the schedule time when the applicant approaches authority verify identification documents with original. After verification of user documents admin go to Verification link and enter user Registration No. On base of Registration No admin get user all details. Admin take user Retina scan and compare with government RETINA table. Human retina is unique. If applicant retina differs with the database of all other retina then application will be clear and in other case its becomes clear that particular applicant had already obtain passport in the past and in that case legal remedy will take its on course of action. After process of user verification admin will go to next step of passport creation. For that admin click on Passport Process link with use of sophisticated hardware face image and fingerprint will taken under supervision of compliant authority and saved for further use when admin click on Create Share. When click on Create Share button that time Visual Cryptography applied on three biometric and it create two meaningful shares. From those two shares share 1 as face image will stamp on hard copy of passport when its generate and share 2 as retina image store in RETINA table for future use.

In the end passport is created in the system and applicant hard copy also prepared for delivery to user. Now user view in Passport Status of his passport is ready for collection. At this stage all the relevant information of this passport will be available for on ward verification at database and passport verification center of various airports and countries embassy. Whenever identification of passport holder is required at admin level Identification option is selected for process. In that Enter Passport No, Current Fingerprint image, Passport Photo scan image which is share 1 and get Retina image from RETINA table which is share 2 and then after click on Identify button. When admin click on Identify button that time share 1 and share 2 stack and Fingerprint image will revealed that compare with Current Fingerprint image. If both fingerprint images matches then its revealed that user passport identification perfect otherwise it is rejected.

A. Algorithms

```
If USER LOGIN link clicked then
   Enter user name and password
Else if Sign up user clicked
   Enter email id as username, password and confirm password
Else if  REGISTRATION link clicked then
   Enter User details
Else if APPLICATION STATUS
    Passport progress
End if

If ADMIN LOGIN link clicked then
   Enter user name and password
Else if REQUEST DETAIL clicked then
   View Requested User list
    Edit user details
    Delete user details
    Send Registration No
    Set status of user passport

Else if VERIFICATION clicked then
   Enter registration no
    Enter user retina     scan
    Click on verify button
       If  Compare user retina with Retina database then
                User had already obtain
        Else if
                Applicant clear
       End if
                Add Retina in table
Else if PASSPORT PROCESS clicked then
     Enter registration no
     Enter Face image
     Enter Fingerprint
     Add user biometrics
     Click on Create Share button
    Create two shares share 1 face image and share 2 retina scan
    Store Share 1 and share 2 in database
    Share 1 for hard copy of passport
    Share 2 for Identification in future
Else if IDENTIFICATION clicked then
    Enter Passport no
    Enter current fingerprint scan
    Scan share 1 from passport
    Get share 2 from Database
    Stack share 1 and share 2 revealed secret image fingerprints
    Compare click button
          If compare current fingerprint and revealed fingerprint then
                Passport identification perfect
     Else if
                 User Rejected
     End if
End if
```

Above IDENTIFICATION procedure will apply in all Embassies and airport.

IV CONCLUSION

Today in information edge, when world is becoming global village and security aspect is more important to isolate anti –social elements, it is required to find out innovative methods for foolproof E-Passport. As retina is sustainable unique biometric, it is very useful for perfect identification of a particular passport holder with use of Visual Cryptography. We can explore methods with more research in other card also.

References

[1] Moni Naor and Adi Shamir, “Visual Cryptography”, advances in cryptology– Eurocrypt, pp 1-12,1995.

[2] Ateniese C., Blundo C., De Santis A. and D. R. Stinson, Visual cryptography for general access structures, accepted for publication in Information and Computation. Also available at http://www.eccc.uni-trier.de/eccc as TR096-012.

[3] Z. Zhou, G. R. Arce, and G. D. Crescenzo, "Halftone Visual Cryptography," IEEE Trans on Image Processing, to appear in 2006.

[4] Blundo C., De Santis A. and D. R. Stinson. On the contrast in visual cryptography schemes Manuscript. 1996. Available at ftp://theory.lcs.mit.edu/pub/tcryptol.96-13.ps

[5] Young-Chang Hou, Visual cryptography for color images, 2003 Pattern Recognition Society. Published by Elsevier Science Ltd.

[6] S. Droste, New results on visual cryptography, Crypto '96, Springer-Verlag LNCS Vol. 1109, 1996, 401-415.

[7] CHING-NUNG YANG, CHI-SUNG LAIH, New Colored Visual Secret Sharing Schemes, Designs, Codes and Cryptography, 20, 325–335, 2000

[8] S. Cimatoa, R. De Priscob, A. De Santisb, Colored visual cryptography without color darkning, Theoretical Computer Science 374 (2007) 261–276, www.elsevier.com/locate/tcs

[9] Matsumoto T., Human-computer cryptography: an attempt , in A CM Conf. on Computer and Communication Security , ACM Press, Marc h 1996, 68-75.

[10] InKoo Kang, Heung-Kyu Lee, Gonzalo R. Arce, Color Extended Visual Cryptography Using Error Diffusion, IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 20, NO. 1, JANUARY 2011

[11] D. Naccache, Colorful Cryptography - a purely physical secret-sharing scheme based on chromatic fillters , in Coding and Information Integrity , French-Israeli workshop, December 1994.

[12] Naor M. and A. Shamir, Visual Cryptography II: improving the contrast via the cover base , Cam bridge Workshop on Cryptographic Proto cols, 1996. A full version is available at ftp://theory.lcs.mit.edu/pub/tcrypto/96-07.ps

[13] Rijmen V. and B. Preneel, Efficient colour visual encryption or `shared colors Presented at the rump session of Euro crypt '96. Also available at http://www.esat.kuleuven.ac.be/~rijmen/vc/

[14] Rubin A. D., Independent one-time passwords, Computing Systems, The USENIX Association, Vol. 9, No. 1996, 15-27.

[15] Hsien-Chu Wu, Hao-Cheng Wang, and Rui-Wen Yu, Color Visual Cryptography Scheme Using Meaningful Shares, 2008 IEEE Computer Society.

[16] E. Myodo, S. Sakazawa and Y. Takishima, VISUAL CRYPTOGRAPHY BASED ON VOID-AND-CLUSTER HALFTONING TECHNIQUE, 2006 IEEE.