Visual Cryptography for Biometric Privacy

Suprabha [1*], Ganesh V N [2*], Shravan Kumar [3*], M B Sachin [4*], Sooraj Shetty [5*]
Dept. of Electronics & Communication Engineering
Mangalore Institute of Technology & Engineering, Moodabidri, India

***Abstract* — Cryptography secures the data during the interaction between different systems. "Biometric", is used for authentication. The attackers may use the opportunities to attack the data within the database. Therefore, the security of biometrics is of high importance. In this idea, a private image is bifurcated into two shares of images and these images to be displayed when the two share images are available together; photos of the sole share cannot reveal the identity of the actual image. To achieve this, Visual Cryptography is used. There are various dimensions on which VCS performance relay, i.e., accuracy, brightness, pixel widening, security, computer complexity, productive sharing is logical or pointless, a kind of private image. This process encrypts a private image into stocks so that it can collect a sufficient number of shares to produce a private image. This project uses VC of colored images in a biometric application.**

Keywords — Biometrics; Visual Cryptography; VCS; Private Face Image.

I. 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. It has created an atmosphere where information is easy to share, clone and modify. Security has become an important factor while communicating, this is due to the presence of hackers waiting for an opportunity to gain access to private data. The computer performs cryptographic functions and from this point, the process becomes fast and secure.

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. There are many techniques in biometric that are available such as fingerprints, retina, face, iris, palmprint, hand vein, voice, signature, keystroke, hand geometry and facial thermogram etc. 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, "Visual Cryptography" is used. In Extended VC, shared images are designed to contain sensible cover images, thus integrating VC and biometric security techniques. At first, this method was used for white and black images but later stated for colored images as well.

II. LITERATURE REVIEW

According to Ref. [1], 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.

According to Ref. [2], the foundation for VC was laid. It assumes that the message is a combination of two elements i.e., white and black pixels. It has a problem of pixel-expansion, i.e., the size of the original message is not the same as the received message.

According to Ref. [3], the paper contains the proposed encryption techniques without the expansion of the pixel and the concept of shared key. The secret share is divided into 2-3 shares and encrypted. Using a key, shares are generated. The results in this paper highlight the fact that system security is highly dependent on the shared key and the total number of shares needed to update the confidential image.

According to Ref. [4], in the 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.

According to Ref. [5], a method is used to create a visual sharing of Visual cryptography, original color rendering (RGB) and 2 shares are created and those are encrypted and then decrypted. Used with MATLAB code and RSA algorithm. This results in good quality RGB color images.

According to Ref. [6], various aspects of VC are discussed. Criteria used to evaluate the efficiency of visual coding systems are explained. Significant use of VC has also been summarized in the study. In this case it suggests that during the encryption phase, the user can see the secret obtained through their detection system, without the intervention of equipment.

According to Ref. [7], the paper suggests an algorithm i.e., the Floyd Steinberg dithering algorithm which is used to manipulate the code of 256-bit image to low code image and for information sharing RGB image is used. In place of the dithering algorithm, we use a half toning process.

According to Ref. [8], the paper suggests an algorithm i.e., a blowfish algorithm for encrypting a data file. This algorithm requires less memory. Each cycle contains XOR functionality and function. Each cycle contains important extensions and data encryption. Blowfish can access active data encryption. Ideal for applications where the key does not change constantly, such as a link.

According to Ref. [9], 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.

According to Ref. [10], the paper suggests how the biometric data is protected from various attacks by splitting the enclosed secret image into 2 separate sheet images so that the image can be reconstructed only if two shares are available together. Enhancing the expansion pixel feature will increase share storage requirements.

III. PROPOSED METHOD

Biometrics can be used to authenticate a person's identity. The two stages of biometric systems are registration and recognition. The first step involves extracting the feature and pre-processing. The features are stored as templates on the database. Therefore, Visual Cryptography is used. It is a private sharing system where we can recover the privacy of any k-share image which is piled together. The entire image contains Red, Blue and Green of 8-bit colours each.

A. Working

This proposed method is divided into 3 parts, namely Image Encryption, Image Decryption and Face Matching. There are many ways we can continue this process. VC can be categorized on the basis of embedded images and logical performance during resharing. Based on the included images can be categorized as binary images and Grayscale / colour

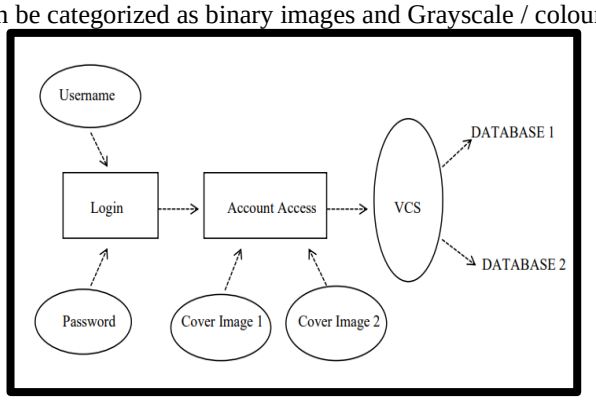


Fig. 1: Data Flow diagram for the Proposed System

scales and based on logical operation OR based and XOR based. Here Halftoning "Floyd Steinberg Dithering Algorithm" for image capture and Blowfish Algorithm is used 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.

B. Encryption

Every image consists of 3 shares, RGB, hence each image is divided into 3 shares. 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.

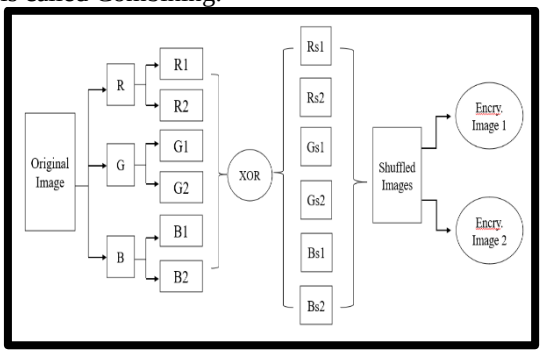


Fig. 2: Encryption method

C. Floyd- Steinberg Dithering Algorithm

The Floyd-Steinberg algorithm is basically an image classification algorithm, which is used to manipulate image tools. It uses image separation using the error distribution process, which means it adds the remaining pixel quantization error to nearby pixels. Dither is commonly used to process both audio and video data. The pixels of the distribution coefficient have a feature i.e., if the actual pixel value is exactly the same as that of the closest colors, the combined result is a test board pattern. The structure is used in the VC sharing process.

D. Decryption

The 2 randomly generated images are chosen to obtain the

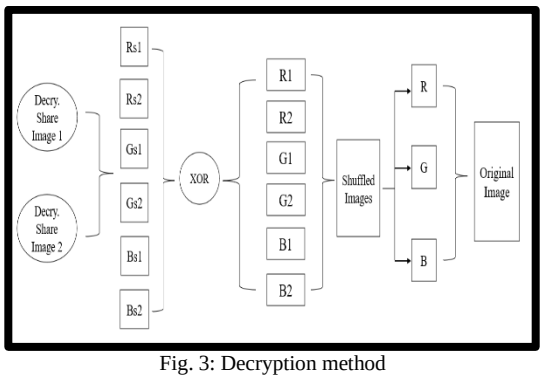


Fig. 3: Decryption method

decrypted image i.e., the original image. Next process is face recognition/matching, where it matches the original image with the decrypted image and checks for the similarity.

E. Face Matching

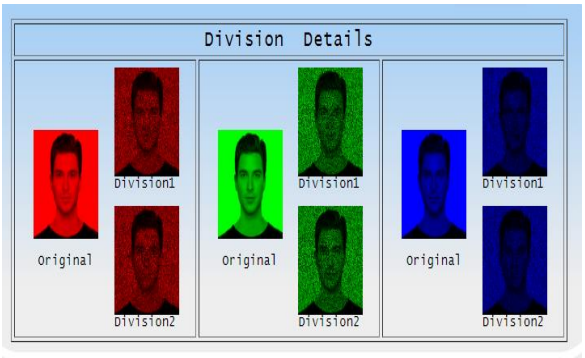
After the encryption and decryption process, verification of the image is necessary. This is done through RANSAC method. It is used to detect the face edges which is helpful for the detection and face verification process.

II. RESULTS AND DISCUSSION

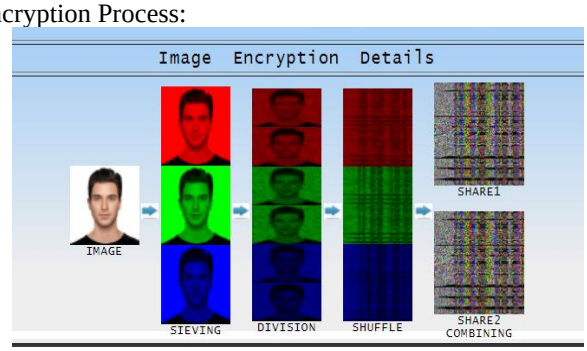
1. A. Encryption Process

Source Image: image.png
Source image used:

Number of shares generated: 6
Image Division:



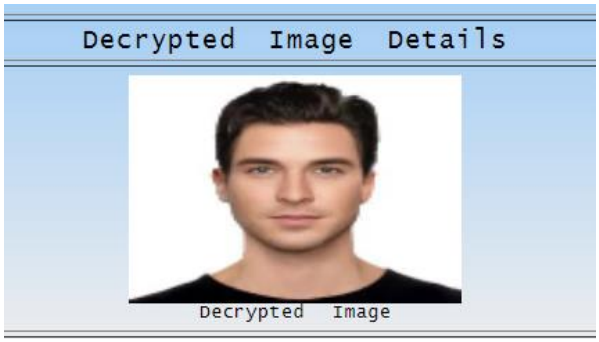
Encryption Process:



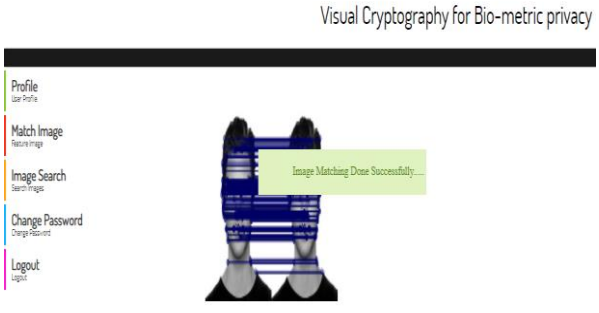
2. B. Decryption Process

Number of shares used: 6

Reconstructed (Decrypted) Image:



3. C. Face Matching



III. CONCLUSION

VC is basically an encryption method which has a merit of decrypting encrypted images rather than cryptographic computations. The significance of VCS in enhancing the security and integrity of secret information has also been considered. The proposed system is done with Floyd Steinberg and the blowfish algorithm.

ACKNOWLEDGMENT

The authors are thankful to Mr. Ganesh V N, our internal guide, Mangalore Institute of Technology & Engineering for his constant support and guidance. Thank you to the professors and friends for helping us.

REFERENCES

[1] Arun Ross, Asem Othman, “Visual Cryptography for Biometric Privacy”, IEEE Transactions on Information Forensics and Security, VOL.6 No.1, MARCH 2011.
[2] Naor, M. and Shamir. A, “Visual Cryptography” EUROCRYPT 1994. Lecture Notes in Computer Science, Vol. 950. Springer, Berlin, Heidelberg (1999).
[3] Shefali Arora & M.P.S Bhatia, “Challenges and opportunities in biometric security: A survey”, Information Security Journal: A Global Perspective (2021).
[4] Jeng - Shyang Pan, Tao Liu, Hong-Mei Yang, Bin Yan, Shu-Chuan Chu, Tongtong Zhu, “Visual cryptography scheme for secret colour images with colour QR codes”, Elsevier November 2021.
[5] Jyoti Tripathi, Anu Saini, Kishan, Nikhil, Shazad, “Enhanced Visual Cryptography: An Augmented Model for Image Security”, (ICCIDS 2019), Published by Elsevier B.V.
[6] M. Karolin and T. Meyyappan, “Secret Multiple Share Creation with Color Images using Visual Cryptography”, April 4-6, 2019, India, IEEE.
[7] M. Karolin, T. Meyyappan, “Image Encryption and Decryption using RSA Algorithm with Share Creation Techniques”, ISSN: 2249 – 8958, Volume-9 Issue-2, December 2019.
[8] P. Punithavathi & S. Geetha (2017), “Visual cryptography: A brief survey”, Information Security Journal: A Global Perspective, 26:6, 305-317 (Taylor & Francis).
[9] M. Karolin, Dr. T. Meyyappan, “RGB Based Secret Sharing Scheme in Color Visual Cryptography”, Vol. 4, Issue 7, July 2015, DOI: 10.17148/IJARCCE.2015.4734.
[10] Apurva A. Mohod, Prof. Komal B. Bijwe, An Image Database Security Using Multilayer Multi Share Visual Cryptography: A Review, ISSN 2319 -4847, Volume 3, Issue 10, October 2014.
[11] Ms Neha Khatri – Valmik, Prof. V. K Kshirsagar, “Blowfish Algorithm”, ISSN: 2278-8727Volume 16, Issue 2, Ver. X (Mar-Apr. 2014), PP 80-83.
[12] Atul Sureshpant Akotkar, Chaitali Choudhary, “Secure of Face Authentication using Visual Cryptography”, International Journal of Innovative Science and Modern Engineering (IJISME) ISSN: 2319-6386, Volume-2, Issue-5, April 2014.
[13] Shubhangi Rajanwar1, Shirish Kumbar2, Akshay Jadhav, “Visual Cryptography for Biometric Privacy”, International Journal of Science and Research (IJSR), ISSN: 2319-7064, Volume 3 Issue 12, December 2014.
[14] N. Askari, H.M. Heys, and C.R. Moloney, “An Extended Visual Cryptography Scheme Without Pixel Expansion for Halftone Images” (2010).
[15] Bhagyashri P. Kandalkar, Gopal D. Dalavi, “Development of Visual Cryptography Technique for Authentication using Facial Images”, IJSR, ISSN: 2319-7064, Volume 4 Issue 12, Dec 2016.
[16] Dr. D. Devakumari MCA., M.Phil., PhD.1, K. Geetha, “A Survey of Visual Cryptographic Method for Secure Data Transmission”, ISO 3297:2007 Certified Vol. 6, Issue 6, June 2017.
[17] Tiwari, Meher Gayatri Devi; Kakelli, Anil Kumar. “Secure Online Voting System using Visual Cryptography”, Walailak Journal of Science &Technology Vol 18, Issue 15, January 2021.
[18] Mr. Ravi Kumar, Ms. Namrata Singh, “A survey based on Enhanced the Security of Image using the combined techniques of steganography and cryptography”, International Conference on Innovative Computing and Communication (ICICC 2020).
[19] Santhi, B K.S. Ravichandran, A.P. Arun and L. Chakkrapani,” A Novel Cryptographic Key Generation Method Using Image Features”, Research Journal of Information Techology 4(2):88-92, 2012.
[20] Anantha Kumar Kondra, Smt. U. V. RatnaKumari, “An Improved (8, 8) Color Visual Cryptography Scheme Using Floyd Error Diffusion”,

in International Journal of Engineering Research and Applications, Vol. 2, Issue 5, September- October 2012, pp.1090.

[21] L. N. Pandey and Neeraj Shukla, "Visual Cryptography Schemes using Compressed Random Shares", in International Journal of Advanced Research in Computer Science and Management Studies, Volume 1, Issue 4, September 2013, pp:62 – 66.

[22] M. Karolin, Dr. T. Meyyappan.SM. Thamarai, "Image encryption and decryption of color images using visual cryptography" International Journal of Pure and Applied Mathematics, Volume. 118, No. 8, 2018, 277-281.

[23] Sozan Abdulla, (2010) "New Visual Cryptography Algorithm for Colored Image" Journal of Computing.

[24] R. Floyd and L. Steinberg, "An adaptive algorithm for spatial greyscale," SPIE Milestone Series 154, pp. 281–283, 1999.

[25] Ateniese, G., Blundo, C., Santis, A., & Stinson, D. (2001), "Extended Capabilities for Visual Cryptography. Theoretical Computer Science, doi:10.1016/S0304-3975(99)00127-9.

[26] Manika Sharma & RekhaSaraswat, (2013) "Secure Visual Cryptography Technique for Color Images Using RSA Algorithm", International Journal of Engineering and Innovative Technology (IJEIT) Volume, 2.

[27] Ram Gopal Sharma, Priti Dimri, Hitendra Garg, "Visual Cryptographic Techniques for secret image sharing: A Review", Vol 27, 2019 (Taylor & Francis).