ISSN 2347 - 3983

Volume 8. No. 3, March 2020

International Journal of Emerging Trends in Engineering Research

Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter06832020.pdf

https://doi.org/10.30534/ijeter/2020/06832020

Attestation Using Visual Cryptography (3,3) Scheme

Dodda Pratap Roy[1], **Dr. M Jaya Bhaskar**[2]

[1] M. Tech Student, Department of CSE (Cyber Security and digital Forensics), KLEF, Vaddeswaram, A.P, India, prataproyd@gmail.com

[2] Professor, Department of CSE, KLEF, Vaddeswaram, A.P, India, jayabhaskar@kluniversity.in

ABSTRACT

Visual Cryptography is a technique in cryptography which is used to encrypt the images and all other visual information. And this cryptography is different from all other cryptographic techniques, because of its decryption process and it is done mechanically. In general, visual cryptography image is encryption is limited up to two shares only. In this paper we propose a complete new and different way of authentication(attestation) which helps to provide more security than other authentication systems by using the Visual Cryptography (3,3) Scheme.

Key words : Attestation, Cryptographic Techniques, Shares, Encryption, Decryption, Shares, Visual Cryptography.

1. INTRODUCTION

In this digital age, technology is developing in many ways like in broadcasting, communications, information sharing, etc. But in some cases, the technology is good but the security to that technology is weak and it may lead to risks while performing operations.

For example, in information sharing there are many ways to share the information in internet and some are insecure, and some are secure. The secured methods mostly use cryptographic techniques to protect the data which was transmitted.

Cryptography is a technique which is used to protect the data. By converting into unreadable format the data will be protected. The word cryptography is divided into two parts called prefix and suffix, in those two prefix and suffix crypt is considered as prefix which means “hidden” and graphy is considered as suffix and it means “writing”.

This technique is used to protect communications and information by using codes and the shared information is only understood by the people who has the codes, and these codes helps to prevent the unauthorized access to data.

In cryptography there are three types of techniques. They are Symmetric Key Cryptography, Asymmetric Cryptography, Hash Functions. And these three follows four feature and the features are Confidentiality, Integrity, Non-repudiation and Authentication.

In Symmetric Key cryptography both the sender and receiver use same key and it is a single key to do both encrypt and decrypt operation on the message which was shared between them and in asymmetric key cryptography both the sender and receiver uses different keys.

In those two keys one key is used to perform encryption and another key is used to perform decryption operation on the secret data. And in hash functions, instead of keys hash value is used for a fixed length to identify the original text.

And these techniques provide some features are, confidentiality means information only accessed by authorized person only. Integrity means information cannot be modified by any other person while transferring between a sender and a receiver. Non-repudiation means information of the sender’s intension cannot be revealed. Authentication confirms that the sender and receiver are real or not [1].

The techniques which are used in cryptography encrypts and decrypts only in text format like a word document or a pdf and other text formats and it doesn’t encrypt the images, signatures etc. To encrypt the images, pictures, signatures etc there another technique and it is called as Visual Cryptography [2].

2. INTRODUCTION TO VISUAL CRYPTOGRAPHY

Visual Cryptography (VC) is one of the powerful cryptographic technique in all cryptographic techniques and it is a quite different one when compare with other traditional cryptographic techniques because of its algorithm.

This algorithm performs encryption only and decryption was done mechanically only with the help of HVS(human visual system). This scheme was developed by Moni Naor and Adi Shamir in 1994 and presented at Eurocrypt ’94. Visual Cryptography encrypts three types of images which are binary (black & white), grey and color.

Visual Cryptography is a cryptographic technique and it is more powerful encryption technique than the other encryption techniques, it divides any visual information into 2 to n number of shares. It is used to encrypt the images, pictures, handwritten pictures, signatures, etc [3].

Here in the encryption the original image will be converted into unidentified images and the images are generally called as shadow images. But in visual cryptography procedure these images are called as shares or parts.

Each part consists equal amount of the original image data in them and the images are unidentified because the images consists only black and white pixels [4].

And the decryption was done only when all the shares of the original image has to be superimposed equally. If the shares don't superimpose equally then the original image doesn't reveal properly.

By using only one part from the 'n' number of shares the original image doesn't reveal any information of original image. The following images figure 1 and figure 2 will show the encryption and decryption of process of visual cryptography [5].

.

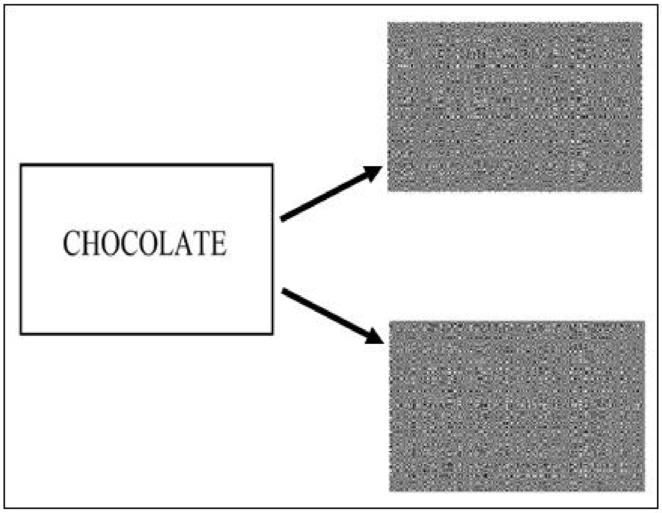

Figure 1: Encryption of Visual Cryptography

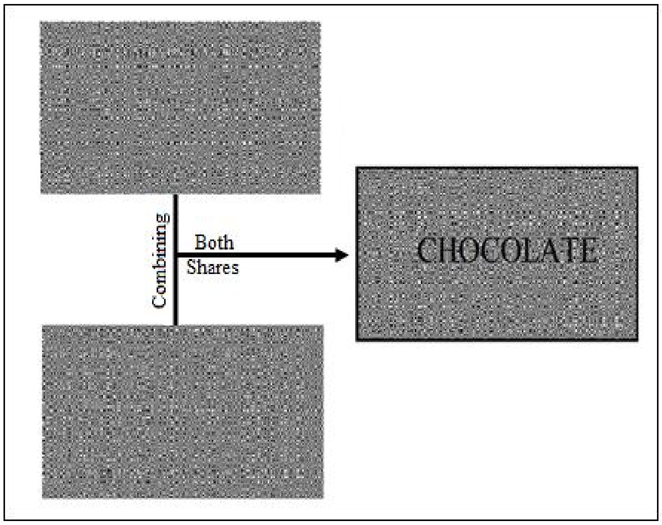

Figure 2: Decryption of Visual Cryptography

3. EXISTING SYSTEM & PROBLEM STATEMENT

The existing system of Authentication using visual cryptography works by using visual cryptography 2 out of 2 scheme or general visual cryptography scheme. Here in this scheme the original image is encrypted into two equal shares and the shares are called as Share1 and Share2.

In those two share, the data of original image is stored equally and to reveal the original image all the shares are needed without any one of the shares the image doesn't reveal. And to decrypt the original image the two shares has to be superimposed equally and then the remaining work of decryption was done by human visual system. And it is shown in figure 3.

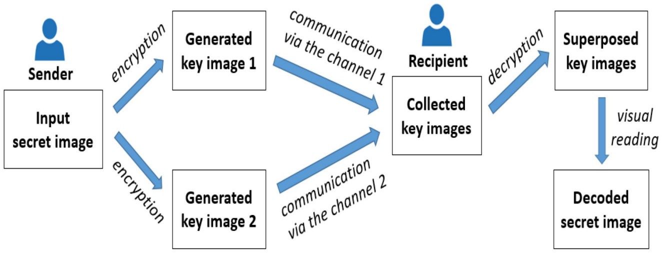

Figure 3: General Procedure of Visual Cryptography 2 out of 2 Scheme

3.1 Encryption of Existing System

In the encryption of 2 out of 2 scheme, the pixels are divided into two equal parts and that was done by performing relative difference and contrasts of two matrices with size of 2X4, because 2X2 matrices may leads to horizontal or vertical distortion which has the binary values of black and white pixels [6].

3.2 Decryption of Existing System

In the decryption process, the shadow images which are called share1 and share2 are superimposed and those two share consists only black and white pixels. When the two shares stacked together the following cases will happen to reveal the original image:

- If the pixel of share1 is black and pixel of share2 is white, then in the original image the pixel will be black.
- If the pixel of share1 is white and pixel of share2 is white, then in the original image the pixel will be white.
- If the pixel of share1 is white and pixel of share2 is black, then in the original image the pixel will be black.
- If the pixel of share1 is black and pixel of share2 is black, then in the original image the pixel will be black.

The following image figure 4 will show how the decryption process will be done on both black and white pixels in the decryption process. And this operation will be done after the user place his card on the scanner [7].

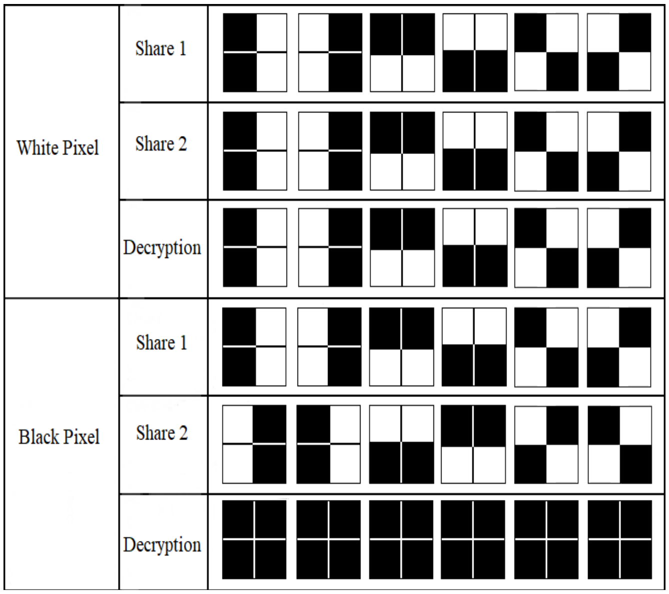

Figure 4: Decryption procedure of both black & white pixels

3.3 Limitation and Problem in Existing System

In the existing system it uses 2 out of 2 visual cryptography (VC) scheme there is a limitations, that is while transferring the images to user and the server a bit of noise will be generated from the shares.

By the help of that noise any attacker who monitor data transactions can identify easily that there is a content is transferring in a hidden format. Here in 2 out of 2 visual cryptography scheme each share consists half of the data so the noise frequency of the shadow images will be more so the attacker can easily identify and the sender and receiver.

And there is a possibility of compromising the receivers between them and tie up with the third person who want to steal the information or may be the third person who want to steal the data can influence them to reveal the original image from the shares.

And another limitation in the decryption process of this scheme is the images which are encrypted, are stored in system dump files and they can reveal secret image easily with the help of the image overlapping tools and photoshop techniques and also be done by some programs which helps to overlapping the shares and the operation of these programs is shown in figure 5.

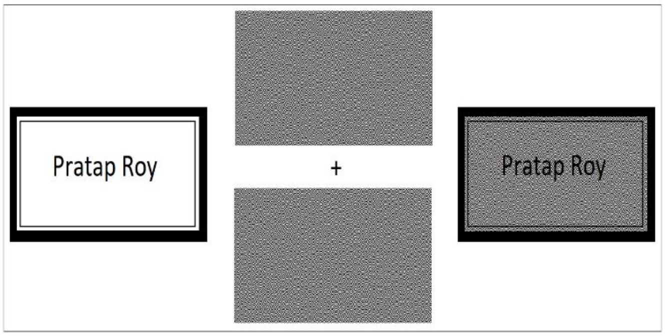

Figure 5: Result of applying a program on VC 2 out of 2 scheme

4. PROPOSED SYSTEM

In the proposed system, the secret code is stored in original image and it is encrypted into three parts equally just as shown in the figure 6, and without anyone of those three shares the original image wasn’t revealed and in authentication process attempt will be failed.

If the three images are found in system dump then also there is no problem with it because any image overlapping tools or any other technique will never work because the techniques which are applied on visual cryptography 2 out of 2 scheme is not easy to apply on this scheme visual cryptography 3 out of 3 scheme.

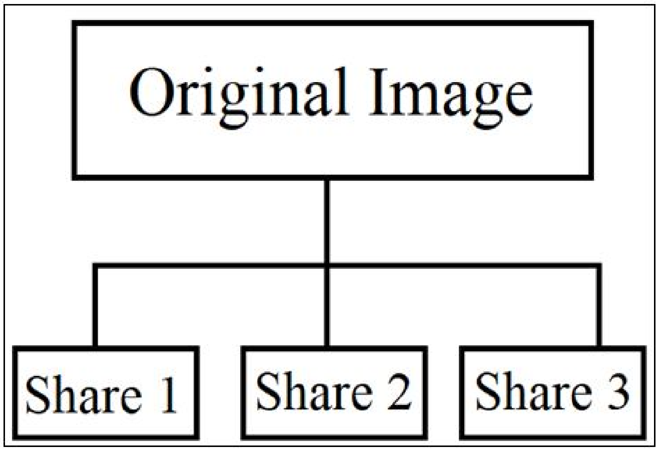

Figure 6: Encryption Structure of Visual Cryptography 3 out of 3 Scheme

Here in this scheme the original image will be divided into three equal shares and distributed. To reveal the original image, all the three shares are needed and without any of those three shares original image doesn’t reveal or decrypt. Even with only any one of these three shares, decrypting of original is not possible.

And with any two of the three encrypted shares, decryption is not possible. In these share all pixels are divided into four sub pixels and theses subpixels are equally filled with black and white colors in six different patterns which are shown in first line of figure 4.

At the time of decryption pixels of the real image are will form. Black pixel consists all the four subpixels in black color and white pixel consists both black and white in the four subpixels equally.

Here also the whole decryption process was done mechanically by the human visual system only. And there is no special algorithm is derived to perform decryption process for this technique and doesn’t need any other computational procedure or other cryptographic knowledge to perform decryption process [9].

4.1 Creating the Encrypting System

In this scheme all the six patterns which are shown in Fig4, are used in two matrices to generate shares and first matrix is ¾th black and the second one is completely black. Let's consider two matrices and call them as S^0 and S^1 and are as follows:

$$S^0 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

$$S^1 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

In above matrices the six patterns which are possible to insert black pixels in a 4 subpixel are used, and in each matrix contains a horizontal, a vertical and a diagonal patterns are stored.

And now calculate the relative difference and is consider as α, and contrast is considered as β. And the relative difference and contrast's results are as follows for the matrices in 3 out of 3 scheme.

$$A = 1/4$$

$$\beta = 1$$

The values of relative difference and contrast shows that the matrices S^0 and S^1 met the conditions of general visual cryptography.

And from the two matrices two matrices are formed C_0 and C_1. In these two C_0 is formed to encode white pixels and C_1 formed to encode black pixels. And the layout of the matrices C_0 and C_1 are as follows:

$$C_0 = \left\{ \pi \left(\begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \right) \right\}$$

$$C_1 = \left\{ \pi \left(\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \right) \right\}$$

In the matrices π means permutation and here the matrices were permuted the columns in the matrices of S^0 and S^1. After permuting these two matrices they give up to 24 new matrices as a result.

By using these permutations, the shares are created and are divided into three parts. And the program is applied on image and it encrypts the image into three parts and are as follows with original image [10].

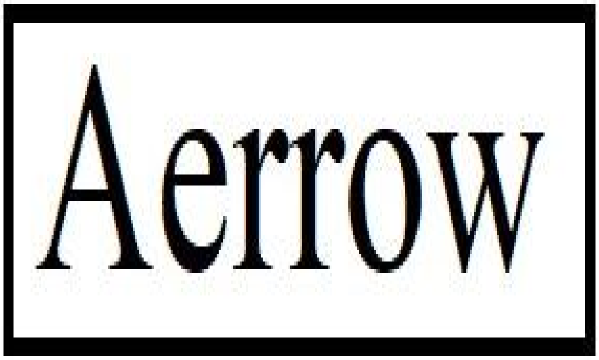

Figure 7: Original Image

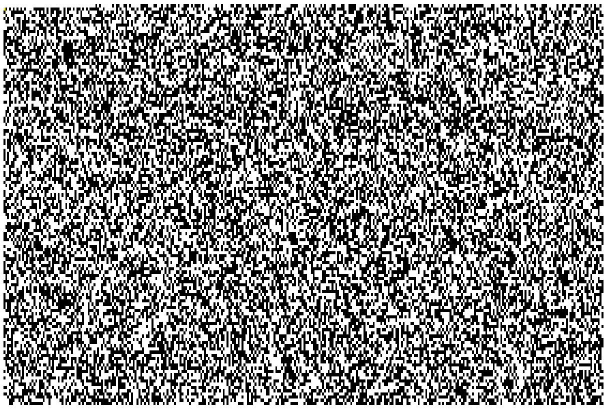

Figure 8: Share 1 of Original Image

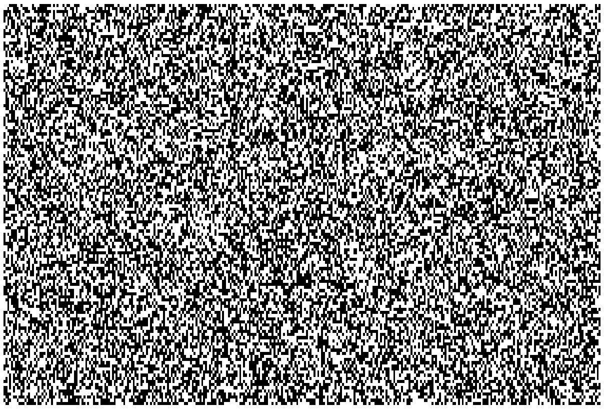

Figure 9: Share 2 of Original Image

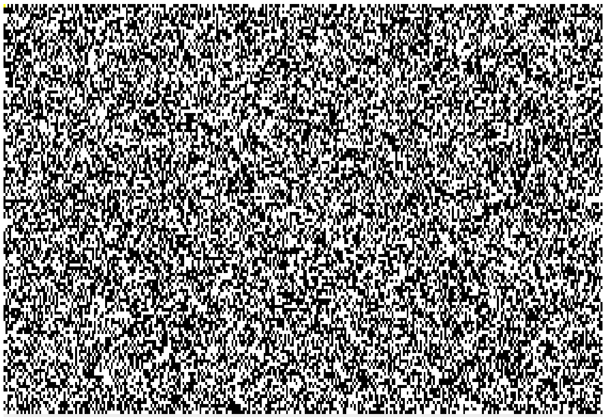

Figure 10: Share 3 of Original Image

4.2 Working of the Proposed System

In the original image it contains a secret code to access an important authentication and the image is distributed to three important people. To access that 3 part are needed because the 3 parts can reveal the secret code in the original image.

If any one of the image is replaced, then the users fail to authenticate, if the user fail to authenticate then the system will be locked for next 24 hours.

And the working of this authentication system is a follows:

- Authentication will be distributed to three individual persons and the three persons are the user, security chief, and the manager, without any one of them.
- And no two person in these three can never get access.
- The access will only give after placing the three cards which are given to those three in their places in the system.
- And then the scanner scans the revealed image and compares the image with the original one and then access will be granted.
- If the cards are used in a wrong way like using the same card to get access the image will not revealed and the authentication will be failed.
- Even if the cards are misplaced the system will warns the user and then gives two more time to authenticate

4.3 Inside Work of the Authentication

Here in this authentication the user need given key card with the remaining two share which are carried by manager and security in charge to get access. To get the authentication all the three users has to place their given key shares has to place them on the scanner of the authentication system.

After placing the three cards on the scanner, the scanner scans the three cards and overlaps them as per place order. And the three cards are shown in figure 8, figure 9 and in figure 10.

After Scanning the cards the scanner generates the decrypted image and then it calculates the hash value of the generated image from the cards and compares the hash value with the original image's hash value.

If the hash values are matched the access will be granted if not the access will be declined. And the decryption done in scanner is shown in the figure 11.

If the user uses only two share from the three shares to get access the system doesn't allow the user to get access even if any one of the three cards is used again in the place of another card the system will be locked and declines the user access request for some time.

The result of this scheme is only done by mechanically with the help of human visual system and to decrypt the user need all the three shares of original image which were shown in figure 8, figure 9 and in figure 10.

And the decryption wasn't done with any two of those three shares. To see or to decrypt the original image user has to use all the three shares and also has to overlap the shares one by one in order and equally to be imposed then only the image will be decrypted[11].

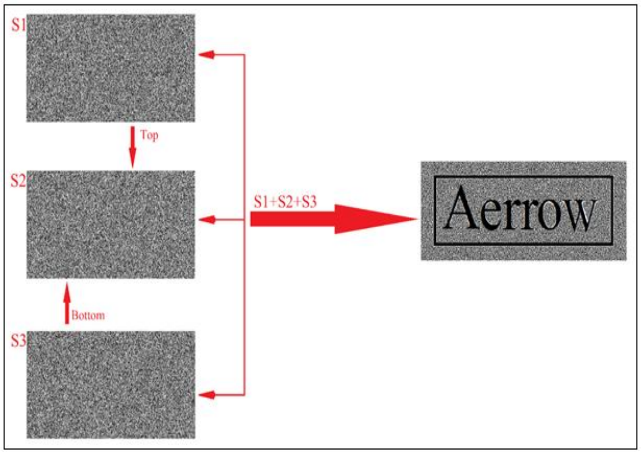

Figure 11: Decryption Procedure of Visual Cryptography with all the three shares

5. COMPARISON BETWEEN EXISTING SYSTEM AND PROPOSED SYSTEM

The proposed attestation system is far better than the existing authentication system which works using Visual Cryptography is a bit less secured because it works as key card authentication, if anyone gets the card, they can easily get the users authentication.

The difference between the existing authentication system and proposed attestation system are quite different because in the existing the user doesn't need any other person for the authentication.

But in the proposed system user needs two more persons to complete the authentication of the user with three cards and it is used to provide security to the most powerful lockers and bank lockers.

Authentication of the both systems is compared, the existing system is faster than the proposed system, but the proposed system is very secured than the existing system. And the encryption of the both the systems is powerful and strong encryption breaking the encryption of the systems is highly impossible.

The encryption of the Proposed system is faster than the existing system, and the proposed system encrypts the image into three parts equally with more security than the existing system.

The decryption of the existing system is possible if the encrypted parts are identified and the decryption of proposed system is not possible even when all of the encrypted parts of the image is identified. And the comparison between both existing system and proposed system is as shown in the following table.

Table 1: Comparative Analysis between Existing system and Proposed system

Method	Attestation	Encryption	Decryption
1.Authentication using VC (978 – 1 – 467349 - 4/15)	Less than 10 Seconds	1.42 Seconds	5 Seconds (Decryption with Overlapping Tool)
2. Proposed System	Nearly 10 Seconds	1.08 Seconds	Decrypted image will be created at the same time of Encryption and it will be stored in hidden format in the Server.

6. RESULT

This attestation provides a powerful security to many confidential areas like banking, secret lockers, etc. And this security system is unbreakable, and this attestation only accessed by the key cards assigned to the user.

In this scheme of encryption user can only understood his part of the operation only but and never understood the operation which was done other side of the process.

And the part which was done by the user is has to place key cards of user and other two main key cards and even the user doesn’t know what was stored inside the key cards, which are used to authentication in this procedure.

In user side the operation goes like this that is first the user has to place his key card in the key slot which is assigned to user and the remaining two were placed by the security and manger.

After placing all the three cards then the three cards generate a unique card and that card was scanned and user gets his authentication and can able to access his locker safely and no other technique never break this system.

The access to the locker which is secured by this scheme provides only way to access is with the key cards only because the key cards consists the encrypted parts of the image which is generated while getting access to the lockers, and safes, etc.

And in the other side of the scheme is inside work and other operations performed by the scanner is the final result of this scheme. This side operation will starts after placing all the key cards in their assigned places on the scanner only.

After placing all the key cards in their place’s scanner scans all key cards one by one and perform overlapping operation and the cards are overlapped one by one just as shown in the figure 11.

Then an image will be formed from all the three key cards and that image contains a secret code which is used to get access to the locker which is the user has to access.

After the completion of overlapping operation the scanner gets the secret image in those three images and then starts hash calculation operation.

In the hash calculation operation the scanner gets hash value of the generated image and stores a side and then move to another operation to provide authentication.

In the other operation the scanner accesses a folder called Original Images and it contains hash codes of the all original images of the key cards which are placed by user on the scanner, and these helps the scanner to identify the user is authorized or not.

After accessing the Original Images folder the scanner gets the related image to the image which is generated after scanning and generates the hash value of the original image.

Then the scanner performs comparison operation between those two hash values of both image which are taken from folder and the one which is generated from the three key cards.

The reason why the hash comparison is used here is the generated image and the original image both contains same hash value and the hash value will change or not.

If any kind of the data is added into the file only otherwise the hash value of any file doesn’t change even after performing basic operation like encryption, decryption, copy, paste, send, share etc.

In the comparison operation both the hash values are compared. If the hash values are matched, then user gets access to the locker. If the hash values are not matched, then user was rejected and alerts the security. If the cards are misplaced the scanner will show error message.

And this whole process will be done in less than 10 seconds whenever the user tries to get access to his locker. And the user can only access his locker only with the key card provided to him.

7. CONCLUSION

Generally Visual cryptography is used to send short messages by adding little work of a cryptanalyst. But in the attestation system it is used to provide a powerful security to identify the unauthorized users while authenticating the user. And this authentication is so useful to hide the data, which is needed at the time of authentication, and when we compare this authentication technique with other normal authentication systems this attestation is very powerful and it is easy to work and provides a better security than other authentication systems. And the great advantage of using visual cryptography scheme in the attestation system is the decryption process visual cryptography scheme and the decryption will only done by human visual system(HVS) and no other cryptographic technique or algorithm will never work on visual cryptography and no other computerised knowledge or any other computer technique will never work on this scheme.

REFERENCES

1. https://www.geeksforgeeks.org/cryptography-and-its-types/
2. http://datagenetics.com/blog/november32013/index.html
3. https://en.wikipedia.org/wiki/Visual_cryptography
4. M. Naor and A. Shamir, Advances in Cryptology-Eurocrypt’94, 1994.
5. An Analysis on Visual Cryptography Midhuna Murali. C, Manjusha. P and 3 Shobana. D
6. http://www.ijceronline.com/papers/Vol2_issue3/E023642646.pdf
7. https://www.slideshare.net/pallavikhandekar212/visual-cryptography-15843873
8. Visual Cryptographic Technique for Enhancing the Security of Image Transaction Akshatha M M, Lokesh B, Nuthan A C
9. An (3, 3)-Visual Secret Sharing Scheme for Hiding Three Secret Data Pei-Fang Tsai, Ming-Shi Wang
10. http://www.cs.jhu.edu/~fabian/courses/CS600.624/slides/VisualCrypto.pdf
11. https://shodhganga.inflibnet.ac.in/bitstream/10603/6102/12/12_chapter%202.pdf