IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-4, April 2019 E-ISSN: 2347-2693

# Visual Cryptography Identity Specification Scheme

**Anmol S. Budhewar[1*], Shubhanand S. Hatkar[2]**

[1,2]Dept. of Computer Science and Engineering, Shri Guru Gobind Singhji Institute of Engineering and Technology, SRTMU, NANDED, INDIA

[*]*Corresponding Author: anmolbudhewar8@gmail.com, Tel.: +00-02462-269240*

DOI: https://doi.org/10.26438/ijcse/v7i4.11481152 | Available online at: www.ijcseonline.org

Accepted: 17/Apr/2019, Published: 30/Apr/2019

***Abstract*—**This paper focuses on the use of visual cryptography for the unique identification of user where different schemes like visual secret sharing schemes, halftone schemes, etc are used. The scheme uses users identifying data to be split into meaningful and meaningless shares. These shares can further be used by merging two shares and reveal the original data content. For additional security of data content, we can use different types of encryption techniques to hide the data content and the same can be retrieved by using the decryption method. The user is identified by the data content hidden in the two shares. One share of the data content can be put on the server side and the second share is at users end. At the time evaluation, one share is shown to the user at the server side and can be matched by the user with given second share of the data content.

***Keywords***—Visual secret sharing (VSS), Visual cryptography (VC), Random grid (RG), Visual cryptography visual secret sharing (VCVSS), Random grid Visual secret sharing (RGVSS)

## I. INTRODUCTION

The safety management to an automated system in order to obtain the applicable targets such as integrity, availability, and confidentiality of information system all along with data transmission over the internet, traditional cryptography schemes were used in previous decades. After long practicing the various cryptographic algorithms then it helps to solve the minimum share problem while the encryption of text and image. The extensive difficulty of cryptography is that a computer is needed for both the process of encoding and decoding, which comes out with wastage of computational resources and CPU execution time.

The eccentricity of the technique is that the human sensory system performs the reconstruction process: no machinery, computing mathematical operations, is needed. Hence, it is often utilized by everyone: once the transparencies are generated and in-camera distributed, science tools or skills don't seem to be required to reconstruct the key image. It is a replacement variety of cryptologic theme, which may decrypt hid pictures with none cryptologic computations. The theme is utterly secure and really simple to implement.

History: The first identified use of a contemporary cipher was introduced by Julius Caesar (100 before Christ to forty-four BC), World Health Organization didn't trust his messenger's once human action together with his governorsshown by R. Arce et.al. [8].

Ex., **Plain Text:** Failure is success if we learn from it. **Cipher Text:**Ldloxuh lv vxffhvv li zhohcuqiurplw.

A wax tablet is a tablet made of wood and covered with a layer of wax. It was used as a reusable and portable writing surface in the 1400 BC.

According to Naor and Shamir, they put a2*2 matrix for the shares. Secret sharing technique by that a secret will be distributed between the clusters of participants. And also the participant is allotted with a bit of a secret. This piece of a secret is thought of as a shareshown by R. Solanki et.al. [2].

Firstly Naor and Shamir introduce the method for a visual secret sharing called as visual cryptography, which can encrypt the classified image into n noise-like sharesshown by M. Naor and A. Shamir et.al. [3].

Table 1: Execs and Cons between VCVSS and RGVSS

| EXECS/ CONS | PROPERTIES | VC VSS | RGVSS |
|---|---|---|---|
| Execs | Knowledge of cryptography | No | No |
| | Computational cost for decryption | No | No |
| | Perfectly secure | Yes | Yes |
| Cons | Contrast | Yes | Yes |

 

| | | | |
|---|---|---|---|
| | Meaningless Shares | Yes | Yes |
| | Pixel expansion | Yes | No |
| | Codebook design | Yes | No |

Unfortunately, neither the generated shared pictures of Naor and Shamir's VCVSS nor the generated random-grids of the standard RGVSS are meaty. In reality, once the shares or random-grids increase, the management becomes problematic; several researchers have paid tidy attention to turning the shares/random-grids meatyshown by T. Chen et.al. [5].

Next section II represent the literature survey, later on it comes with section III represent proposed method, section IV Experimental results.

## II. LITERATURE SURVEY

### *A. Visual Cryptography*

The idea behind dynamic visual cryptography is that increasing the visual cryptography theme. This implies that mistreatment 2 or a lot of shares for the scientific discipline message. It's a replacement sort of scientific discipline theme, which may rewrite hid pictures with none scientific discipline computations. The theme is dead secure and extremely simple to implement. Visual cryptography (VC), planned by Naor and Shamir, may be a paradigm for cryptologic schemes that permits the coding of hid pictures with none cryptologic computation. Notably during a k-out-of-n visual secret sharing theme (VSS), a secret image is cryptographically encoded into n shares. Every share resembles a random binary pattern. The N shares square measure then photocopied onto transparencies severally and distributed among n participantsshown by Shivani Pahuja et.al. [9].

For this afresh visual secret sharing (VSS) theme known as visual cryptography (VC) was developed to safeguard sensitive pictures from rapacious behaviour. For (k, n)are general theme of the edge, a secret image is encrypted into random-looking pictures that are known as shares or shadows. These shares are at the moment distributed to associated participants. To visually reveal the key, any or a lot of shares are needed to stack along. However, any or fewer shadows provide no clue regarding the key.

### *B. Extended Visual Cryptography*

The mechanism behind visual cryptography is to a digital encoding technique for the faster transmission. According to the fig secret image get encrypted by using these two shares share A and share B. In the visual cryptography, we can use it both such as image and textual message.

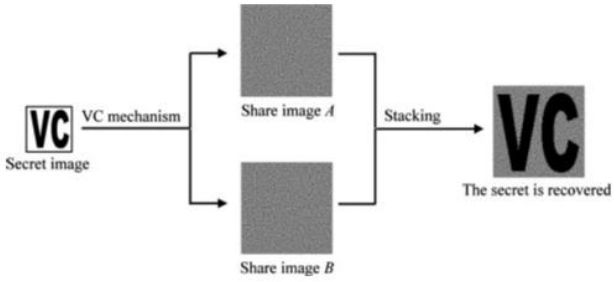


Figure 1: Visual cryptography mechanism

The encryption of image is on the basis of (k, n) visual cryptography scheme in which it uses the (m, n) matrices in a generation of shares. Such matrices are basic Boolean matrices ($C_0$) and ($C_2$). To share a white or black pixel, the dealer randomly selects one row of the Boolean matrix $C_0$ ($C_1$ ) and assigns it to the corresponding share image. The encrypted image is divided into two share and n shares present as per the image size. That referred to as meaningful and meaningless, mostly the meaningful message used for image and meaningless for textual data [7].

The encrypted image is split into 2 (n) share pictures so the key are often disclosed on condition that each the shares area unit stacked along. The mathematician matrices to be sent are often designed as follows:

$$S_1 = [1\ 0\ 1\ 0\ ] \qquad S_2 = [1\ 0\ 0\ 1\ ]$$

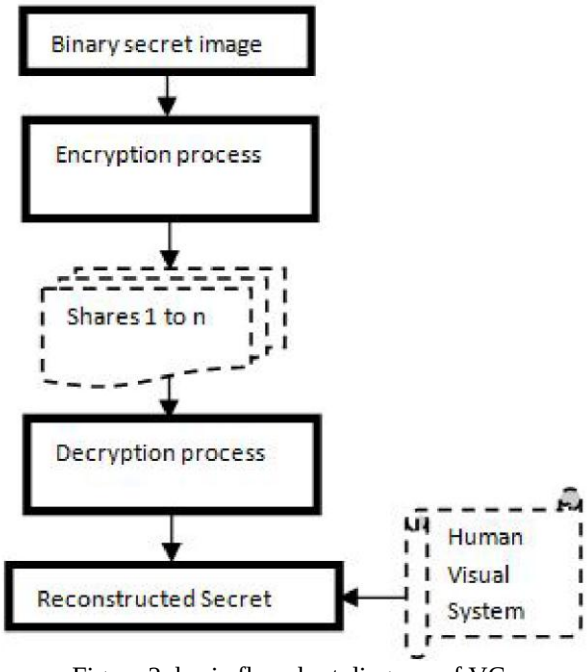


Figure 2: basic flowchart diagram of VC

 

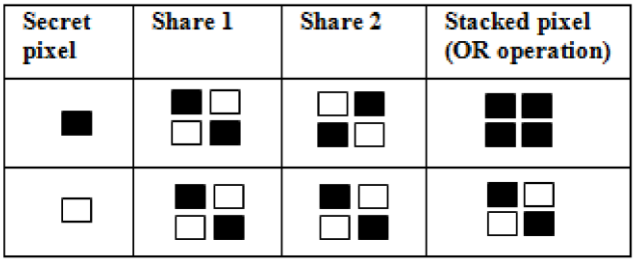


Figure3:(2, 2) Visual Cryptography Scheme (VCS)shown by Sruthy K. Joseph et.al.[4]

Within a secret sharing theme, the key is split into a variety of shares and distributed among n persons. Once any k or a lot of those persons (where k n) bring their shares along, the key is often recovered. However, if k -1 person decides to reconstruct the key, they're going to fail. because of this threshold theme, we have a tendency to usually confer with such a secret sharing system as a (k, n)-threshold theme or k-out-of-n secret sharing, wherever n is that the variety of Total Participants and k is that the variety of Qualified Participants the fundamental model for visual sharing of the k out of n secret image is such that;

- Although any of n participants will reason the first message if any k (or more) of them area unit stacked along.
- No cluster of k-1 (or fewer) participants cannot reason the first message.

The three algorithms explained by Shyu extended Kafri and Keren's gives a thin transmission output. In their start up model, secrete image containing from the picture element which will be R1 and R2 are combined with color. This leads to generation of out of black in black area units and a ratio of five hundredth black in given white areas the two share pictures are stacked within it. In their next algorithm model if the content of picture inside the secrete shared image is white, R1 and R2 are same color, when the picture content inside the secrete image is black then the color of R2 is occupied and shown by Young-Chang Hou et.al. [1]

## III. PROPOSED METHODS

Black appearing probability is calculated and then it analyzes the change in chromaticity in share image and also in stack image further it called a secret image. An area with the black pixel is assigned with very high probability with getting black has a higher density of black pixel. And on the opposite hand, the chance of white constituent as compared to blackness. The density during this space is low therefore and space sounds like lighter.Shown by K.H. Tsaoal. [10]With these 2 possibilities, we will manufacture a dark and light-weight distinction within the image and that is shown within the black and white pattern.

### *3.1 User-Friendly VSS*

The easy VSS methodology is employed to share image ought to show the duvet image on that. There are 2 completely different black element prospects referred to as X and Y, wherever X indicates the black appearing chance once the element within the cover-image is white and Y represents the black-appearing-probability once the element within the cover-image is black. It's clear that X < Y.

1) Those pixels representing the black inside the stacked image are designed the different colors combinations of two shared pictures. The changes are showed by following.
2) When the pixels represents black as two cover-images, where each pixel have Y chance to become black. Two shares black pixels square measure stacked is calculated the chances that can vary from entire overlapping to not covering overlapping the smallest bit, this indicates that appearing probability of black pixels from the areas of stacked image is variance within the Y and 2Y.
3) If white is the color content of two cover-image then the content has X chance to have black. Once the total black pixels with given shares of pictures are stacked then the outcome results may vary from all overlapping to non-overlapping. The smallest bit that represents the black pixels which appearing chance of those areas between the X and 2X. When one of two cover image pixel color is black and the second color is white and the given images are stacked then the probability of black appearing colors in areas of stacked images will be in between X and X+Y.

### *3.2 User Friendly VSS Scheme*

In this sharing scheme, the sharing codebook contains four combinations for both black and white pixels. According to the survey black pixel presenting probability the black and white pixels

Table 2: VSS codebook

| Secret Image | Cover 1 | Cover 2 | Share 1 | Share 2 |
|---|---|---|---|---|
| ■ | ■ | ■ | Y | $\frac{(2*Y-W)}{Y}$ |
| | ■ | □ | Y | $\frac{(X+Y-W)}{Y}$ |
| | □ | ■ | X | $\frac{(X+Y-W)}{X}$ |
| | □ | □ | X | $\frac{(2*Y-W)}{X}$ |
| □ | ■ | ■ | Y | $\frac{(2*Y-Z)}{Y}$ |
| | ■ | □ | Y | $\frac{(X+Y-Z)}{Y}$ |
| | □ | ■ | X | $\frac{(X+Y-Z)}{X}$ |
| | □ | □ | X | $\frac{(2*X-Z)}{X}$ |

 

In the given stack image are denoted by W and Z respectively with the values variations Z and W under various sequences of colors in the cover-image will be between X and 2Yshown by Wei Sun et.al. [6].

### 3.3 *Meaningless Share Image VSS*

The Principal purpose of the insignificant share image VSS technique is that there ought to be obvious distinction between black and white spaces in the stacks image suggestive arrangement of the key image, however such distinction shouldn't be detectable within the shared image that ought to gift a noise like metallic element imagePlace table titles above the tables.

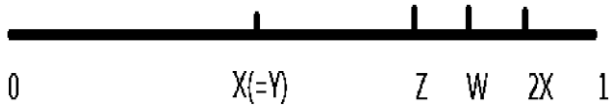


Figure 4:.line-distribution-Probability graph for meaningless vss.

In the condition X = Y, the easy VSS codebook may be reduced to the insignificant visual secret sharing codebook. each share image one and share image a pair of can have X proportion of black pixels, in spite of whether or not the corresponding space on the key image is black or white.

## IV. EXPERIMENTAL RESULTS

There are various examinations were carried out on individual computer system having associate Intel Core i5-2410 two. 30GHz CPU, with 4GB memory exploitation the Windows plate-form. The event language was C#.

**Observation 1: Meaningless Share Image**

In this observation, there are some individual elements are taken such as characters, symbols, etc. In image form that will be rearranged in a grid format. Whose values decided on the W and Z.In order to create the distinction within the stack image a lot of obvious, we tend to set parameter Z adequate X and parameter W adequate 2X.Shown by Young-Chang Hou et.al. [1]

Figure 5 :( Experimental image1) Original Message

Here in the both meaningful and meaningless method is used to share textual and image data.

**Observation 2: User Friendly Share Image**

There is some method in which they use common share technique, share scheme, some use the grid. In my method is somewhat different because it uses only two shares in which the entire message can encrypt. When these two pieces of share get overlap with one another it gets decrypted.

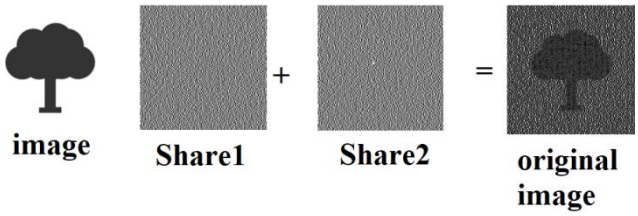


Figure 7: Image encryption using two shares

Figure 6: (Experimental image2) Decrypted Messageshown by Young-Chang Hou et.al.[1]

Table 3: Correlation of the proposed methods and some related methods

| Scheme | Pixel expansion | Codebook design | Meaningful shares | Share scheme | Decryption |
|---|---|---|---|---|---|
| Visual cryptography | Yes | Yes | No | (k, n) | OR |
| Multiple random grids | No | No | No | (n, n) | OR |
| Extended Visual Cryptography | Yes | Yes | Yes | GAS | OR |
| User-friendly | No | No | Yes | (2,2) | OR |
| Generalized Random Grid | No | No | Yes | (n, n) | XOR |
| Random-Grid based VC | No | No | Yes | (2,2) | OR |
| Random Grid based Visual Cryptography using a common share | No | No | No | Modified(2,2) | OR/XOR |

 

## V. CONCLUSION

From the techniques of splitting the data into two shares whether it is meaningful or meaningless we can encrypt the data which may contain images or text. In the same way, we decrypt it using a merger of two sharing and use of this technique in identification is very efficient. The uniqueness can be maintained by sharing one part of an encrypted image and assigning the part with a specific user that maintains the unique identification of the user. Similarly, if we want to evaluate the uniqueness of the user we can match the share assigned to the user with the second share generated at the time of encrypting the data content. This focuses on the effective use of visual cryptography in finding out the respective user related to the share.

## REFERENCES


[1] Y.C. Hou, S.C. Wei, and C.Y. Lin, "*Random- Grid based Visual Cryptography Schemes*", *IEEE* Transactions on Circuits and Systems for Video Technology, VOL. 24, NO. 5, May 2014.

[2] R. Solanki, "*Principle of Data Mining*", McGraw-Hill Publication, India, pp. 386-398, 1998.

[3] M. Naor and A. Shamir, "*Visual cryptography*," in *Proc. Adv. Cryptology-EUROCRYPT'94*, LNCS 950, 1995, pp. 1–12.

[4] S. K Joseph, R. Ramesh , "*Random Grid based Visual Cryptography using a common share*", 2015 Intl. Conference on Computing and Network Communications (CoCoNet'15), Dec. 16-19, 2015, Trivandrum, India.

[5] T. Chen and K. Tsao, "*User-friendly random-grid-based visual secret sharing*", *IEEE* Trans. Circuits Syst. Video Technol., vol. 21, no. 11, pp. 1693-1703, Nov. 2011.

[6] X. Wu and W. Sun, "*Generalized Random Grid and Its Applications in Visual Cryptography*", *IEEE* Transactions On Information Forensics And Security, vol. 8, NO. 9, September 2013.

[7] *http://bookboon.com/en/visual-cryptography-and-itsapplicationsebook.*

[8] Z. Zhou, G. R. Arce, and G. D. Crescenzo, "*Halftone Visual Cryptography*," *IEEE Trans. Image Process.*, vol. 15, no. 8, pp. 2441–2453, Aug. 2006.

[9] S. Pahuja, S. Kasana, "*Halftone Visual Cryptography For Color Images*",International Conference on Computer, Communications and Electronics (Comptelix) Manipal University Jaipur, Malaviya National Institute of Technology Jaipur & IRISWORLD, July 01-02, 2017.

[10] T. H. Chen and K. H. Tsao, "*Threshold visual secret sharing by random grids*," *J. Syst. Softw.*, vol. 84, no. 7, pp. 1197–1208, 2011.


## Authors Profile


**Prof. Hatkar S. S.**

B.E. (Computer Science & Engg.), M.E. Electronics (Specialization in Computer) having 23 years of experience in Academic. Currently he is the Associate Professor at Shri Guru Gobind Singhji Institute of Engineering and Technology, at Nanded. His areas of specialization are Information Security and Theory of Computer Science.

**Anmol S. Budhewar**

Persuing M.Tech. (Computer Networks & Information Security) at Shri Guru Gobind Singhji Institute of Engineering and Technology, at Nanded. And area of interest are Computer Networking and Cryptography.


 