# An Optimization Model for Secure Sharing of Visual Cryptographic Images Generated by Using arbitrary Pixel Stereogram

[1]Divya. R
B.Tech Final Year (IT)
Velammal Institute Of Technology, Panchetti, Tamilnadu, India.
*divyarajabaskar@gmail.com*

[2] Nandhini. A. T [3]Prathyusha. A
B.Tech Final Year (IT)
Velammal Institute Of Technology,India
*atnandhini@gmail.com*
*prathyuakula02@gmail.com*

***Abstract*—** Visual cryptography schemes (VCSs) are the methods to provide data security in network systems by generating arbitrary and non meaningful parts of a original image under consideration. There occurs a issue of transmission loss and also the possibility of the invader attack when the shares are passed within the same network. Previous research have focused on securing the shares in halftone images but the possible risks they lead to are pixel enlargement issues and deterioration of the image quality. Hence a binocular visual cryptography (BVC) and an algorithm for encryption are used to protect the shared pixels in the arbitrary dot stereogram in addition to the other modes of transmission for the generated possible shares. In order to reduce the conveyance threat of the divided parts this paper uses the 2D appearance of the SIRDS in order to use as a envelope for the parts. The algorithm used may modify the arbitrary dots in SIRDS's to equalize the nature of the resultant image. This process is done using the composition guideline of BVCS. Altering the dots may also have a impact on the pixel quality and hence an optimization model based on the quality requirement is used. Finally the shares are passed to the recipients over varied networks.

***Keywords-*** *cryptography, arbitrary dot stereogram, conveyance risk, dot enlargement*

*****

## I. INTRODUCTION

Visual cryptography (VC) proposes the methodology where the single image is encrypted into n shares and these shares are distributed to the various recipients who have authority to hold the original confidential image [1]. Any recipient can decrypt the image only if has 2 or more shares. If there are less number of shares then the proposed threshold for a single recipient then he would not be able to decrypt the image. Accumulating the k dividends reveals the confidential image, that is easily identified by human eye. Current shares which consist of many arbitrary and insignificant images are sufficient for protection of the confidential content but suffer from the high conveyance risk because the attackers may gain the information from the noise that are produced by the insignificant shares and try to seize the shares. This possibility leads to the difficulty of transmission losses and inability to deliver the original content to the intended user. EVC Scheme provided a purposeful appearance for parts to make the shares that are noisy to be feasible for shareholders which still carried the obstacles of being detected by invaders .Here the parts that are imprinted on translucence encompasses many defected images in addition to the poor nature pictures. Parts are smoothly identified by the human visual system and shareholders who dispatch the parts can finely arise the uncertainty of future queries of attacker. Another scheme involved the use of visual cryptographic parts that makes use of half toning method to develop appropriate binary pictures as dividends carrying appropriate visual information. The ocular quality of the picture is preferred than that obtained by extended version. The parts received using such an method can decrease the conveyance risk of the dividends, but it is accompanied with the image enlargement issue and deterioration of the obtained share and images. Hence researches on optimized techniques for safe and efficient transmission of the shares have to be evolved for the participant which also safeguards the quality. Jules developed the arbitrary-dot method, in which the three dimensional structure trespasses the monocular movement and it is seen when stereoscopic amalgam is received. A arbitrary-dot stereogram is a stereo-couple of pictures of arbitrary spots, which when examined with the help of a stereoscope or with the humaneye directed on a notch before or after the images, yields a emotion of depth, in addition to the objects displaying to be before or at the back of the exhibit level. Further studies evolved the development of 3D form of the stereoscopic image by the use of arbitrary dot pattern.

## II. EXISTING SYSTEM

Based on the exploration, VCS with appropriate parts can be splitted into two methodologies: (1) cryptography approaches and (2) embedded approaches. The first idea uses an algorithm to concurrently encrypt a part and afford a valid appearing for the parts. The initial technique needs plotting a firm of basic grid for a specific visual cryptographic parts but it is accompanied with the issue of image enlargement. The

arbitrary grid based approach involves constructing visual cryptographic parts and its extended version. The central intention behind the arbitrary based technique is that it encrypts a confidential picture to the dividends related to a provided probability *a* and imprints cover pictures on the dividends with *(1 −a)* probability. By tuning probability *a*, the given technique can change the ocular elements inserted in the rediscovered image and the parts of an extended visual cryptographic parts. The implanted approach tries to imprint covering pictures in the parts or to secure parts behind covering images. This system suffers from the issue of expansive tabulation and high time complexity. The risk of invaders attack is also high in these cases.

## III. OTHER RELATED WORK

Kai-Hui Lee et al [1] made the study on hiding the (2, num) - num represents the participants taking part, identical dividends produced into the random pixel stereogram. This work also researched on the possibility of hiding the dividends under the made transparencies. A model that defined a series of building rules to obtain the original pictures of the (2,num) binocular cryptography for visual secrets such that the pictures have the highest black and white variance caused by interference in the stereogram. A required picture quality is achieved by modifying the instructions in the building rules along with the parameters used in the model. The best color variation of the recovered system lies between 2<i<10, and the answer produced was in limits of 2.0 to 5.0 with a better clarity of the decrypted image. The results of the experiments proved the flexibility of the proposed (2, num) light dividends system.

N. Askari et al [2] proposed a novel scheme which dealt with the possible exchange of the participant blocks in the images of the half toning process known as the Balancing participants Block Method. The idea that adds novelty to this approach is participants block replacements method produces the enhanced method of balancing the contrast between the black and white pixels in the obtained and working recovered dividend. The SBR production will produce the heavily contrast images since the parts which have the specific number of white and black dots are modified into the overall black parts. Blocks n black and n white pixels regarded as the reserve blocks. In participant's replacement scheme, the two variants of blocks are calculated and revealed by allotting some participants to white and others to black. Although the assignment of participants block invariably to the color contrast blocks may increase the standard of the original secret picture the possibility of attaining the better caliber is by application of the methods and the schemes that follow the intelligent participants exchange methods. Such schemes follow a practice where the features of the genuine picture are considered while altering the participants' blocks. The participants block changing method keeps the proportions of the white and the black dots obtained picture very identical to the stored proportion of the dots in the original secret data produced from the halftone scheme. Hence, the produced picture in close comparison to the authenticated original one on the scales other than colored ones. This work overcomes the disadvantages of the existing half tone techniques.

Zhongmin Wang et al [3] proposed a fallacy diffusion methodology which is a easy half tone method which involves the technique where the sampling mistake at every pixel is removed and again given to the original input. The fallacy on one part is propagated gradually to other part of the grayscale picture through the filter used for the fallacy detection and estimation..The noise that is created due to this process or the high range of frequency in the processing is referred to as the blue noise. In cryptographic scheme which involves half toning, the fallacy is introduced by the encoding of the naïve secret data and is passed to the next subsequent pixels by the help of the scattering filters which prove the existence of the errors. This yields the production of high standard pictorial parts. In a alternate way to the two process method in the existing half tone technique, the work showcased Zhongmin Wang involves the scheme where encoding of the naïve picture in correlation with half tone error scattering..The calculation involved a linear diluting pattern and is accompanied by the scattering quantization. The naïve data is split into non overlapping columns of $A_i * A_n$ .In order to encrypt the secret data, the authenticate information details are evenly distributed in the possible homogeneous level to reach the designated recipients. A cross plotted value for the co ordinate points depicting their relationship A shows that for every halftone part, the cell is chosen in a un predictable manner from zero to one which varies on the value of the native secret picture. The secret data parts of the corresponding halftone cell in the $i^{th}$ share are replaced with the $i^{th}$ row of M. Thus the occurrence of the points in the native secret information in correspondence to the half tone pixel parts can be detected easily before the error slides to the forth coming parts. In this way half tone begins and the shares are secure from losses.

R.Ito et al [4] studied the drawbacks of the conventional VC which include the problem of enlargement of the pixel and the unconventional reduction in the quality of the obtained image. The issue was raised due to the absence of the uniform technique to hide the data into the structures for the random access. He proposed a simpler and systematic approach for the existing design if the used codebook. The decryption of the confidential data in computer or device less situations made use of this solution well. In order to overcome the enlargement of the dots used,, the of a group of vector columns to embed the dividends instead of enlarging dots. The process is ended with the employment of annealing algorithm. The results conducted found that the decrypted images have produced a good and impressing quality when compared to the previous schemes.

Shital B.Pawar et al [5] after analysing the prevailing techniques for half toning combined with dithering voiced a new Thresholding way. Least Significant Dots matching is one of the suitable ways to bury the confidential data into the undercover images which is a part of the stenography schemes..Related works were also investigated that the use of the techniques which are currently in practice for dithering and half toning did not produce the pictures parts of high quality.

Thresholding method for the use half toning produces high contrast images in a best possible method. Left significant dots are the best way to hide the secrets to an image. Their research aims at employing left significant dots steganography with Otsu's method to find an efficient alternative of the existing visual cryptographic system. This method not only increases the visual quality of recovered secret but also gives better results.

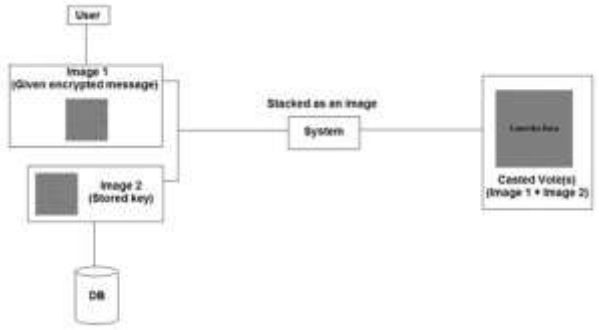
## IV. PROPOSED SYSTEM

We propose *(2,num)*-binocular cryptographic parts with binary confidential picture with *num* participants (*num* ≥ 2*)*, when the involved contributors heap their parts , the underlying . *(*2, *num)*- binocular parts are secured in *num* arbitrary dot stereogram to decrease awareness to raiders during the conveyance phase. The proposed model of encryption procedure consists of three phases. In the initial phase, *num* SIRDS are generated by using conventional formation system. Second phase, is the alteration of the arbitrary dots [6] according to a composition guideline of the *(*2, *num)*- binocular cryptographic parts for securing the binary confidential image. The composition guideline is for securing the confidential image in the SIRDSs securely .The third phase is the transmission of the generated shares in multiple transmission modes involving varied networks. But, collapsing the spots in a stereogram will impede with the humanbrain's capacity to attain the real three dimensional structure in the SIRDS and diminish the ocular quality of the restructured items. Hence, an elaboration technique to search composition guidelines for the *(*2, *num)*- binocular cryptographic parts such that the encryption method yields a confidential parts and the comparison of the reconstructed confidential image can be enlarged, liable to the ocular quality of the stereogram and parts are also protected from invader attacks.

The merits of the proposed system are conveyance with high secured using dot Stereogram pictures and disabling of the possible attacks to the emission of the dividends.

## V. SYSTEM ARCHITECTURE

As mentioned earlier in this paper we use to secure the text without image enlargement. So we propose (2,num)- binocular cryptographic parts that shares a binary confidential image with the shareholders. This will decrease the awareness to invaders during the conveyance phase.




The system architecture is constructed to depict the concept. The diagram below describes about the flow of the data between the sender and the receiver. Initially, the user creates the text or image that he needs to send and by using our proposed technique the encryption of the text is done.

***ENCRYPTION ALGORITHM***

1. $\forall 1 \le i \le n$, **let** $S_i \leftarrow ST_i$
2. $\forall 1 \le y \le h, 1 \le x \le w, p^{L}_{x,y} = 1$, **repeat** Steps 3—10
3. **Let** $b^{ST} \leftarrow H([p^{ST_1}_{x,y} \quad \dots \quad p^{ST_n}_{x,y}])$
4. Generate a random number $\rho$, $0 \le \rho < 1$.
5. **Let** $c \leftarrow p^{SE}_{x,y}$
6. Determinate $b^{S}$ based on $\rho, m^{c}_{b^{ST},0}, \dots, m^{c}_{b^{ST},n}$
7. **If** $b^{S} > b^{ST}$ **then**
   Randomly select $(b^{S} - b^{ST})$ shares where $p^{S_i}_{x,y} = 0, 1 \le i \le n$, and let $p^{S_i}_{x,y} \leftarrow 1$
8. **Goto** Step 2
9. **If** $b^{S} < b^{ST}$ **then**
   Randomly select $(b^{ST} - b^{S})$ shares where $p^{S_i}_{x,y} = 1, 1 \le i \le n$, and let $p^{S_i}_{x,y} \leftarrow 0$
10. **Goto** Step 2
11. **Output** shares $S_1, \dots, S_n$

Based on this algorithm the user's data is encrypted and it is sent to the other side for encryption. Using this algorithm two encrypted images are created. This encrypted message consists of two images namely key and source image and they are used to decrypt the data later. This key image and the source image are sent to the receiver separately.

At the receiver side, the two images are stacked together and checked for the authenticated data. If that overlapped image satisfies the needs then the image will be decrypted at the receiver side. If it identifies any error in the overlapped image then the decryption will not occur rather error will be displayed. By this way we can promote security to the data sent between the sender and receiver.

## VI. CONCLUSION

The overall scheme proposed for the optimization of the conveyance methodologies for secure sharing of visual cryptographic images generated by using arbitrary pixel stereo grams overcome the conflicts of the conventional methods by the use of encryption based parts and varied channels for transmission and a default stored repository. The used arbitrary approach can overcome the obstacles of image enlargement, but it cannot provide high ocular quality dividends and rediscovered images. Hence an improvement model for enhancing the quality is used. Also the embedded approaches can generate etching parts with high ocular quality, reducing the suspicion and emission of an encrypted parts

## REFERENCES

[1] Kai-Hui Lee and Pei-Ling Chiu "Sharing Visual Confidentials in Single Imagearbitrary Dot Stereo grams" IEEE Transactions on Image Processing, Vol. 23, No. 10, October 2014

[2] N. Askari, H.M. Heys, and C.R. Moloney "An Extended Visual Cryptography Scheme without Pixel Enlargement for Halftone Images "26th IEEE Canadian Conference of Electrical and Computer Engineering, 2013
[3] Zhongmin Wang and Gonzalo R. Arce "Halftone Visual Cryptography through Error Diffusion "
[4] R.Ito, H. Kuwakado, and H. Tanaka, "Image size invariant visual cryptography," IEICE Trans. Fundam. Electron, Commun, Comput.Sci, vol. E82-A, no. 10, pp. 481–494, 1999.
[5] Shital B.Pawar, Prof. N.M. Shahane "Visual Confidential Sharing Using Cryptography " International Journal of Engineering Research , Volume No.3, Issue No.1, pp : 31-33
[6] T.-H. Chen and K.-H. Tsao, "User-friendlyarbitrary-grid-based visual confidential sharing," IEEE Trans. Circuits Syst. Video Technol., vol. 21, no. 11, pp. 1693–1703, Nov. 2011.