

Analysis & Design of Secure and Contrast Enhanced Secret Sharing Scheme Using Progressive Visual Cryptography

Shivam Sharma¹, P. Priyadarshni²

Research Scholar (B.E (Hons.), ECE), Birla Institute of Technology & Science, Pilani-Dubai Campus
Department of Electronics & Communication (ECE)

Abstract: Visual cryptography is a system offering arrangement which uses pictures flowed as shares such that, when the shares are stack, a touchy or emit picture is uncovered. As per expanded visual cryptography, the offer pictures are manufactured to hold convincing spread pictures, in like manner giving open avenues to organizing visual cryptography and biometric security routines. In this paper, we propose a plan for halftone pictures that improves the way of the shares produced from discharge picture and the recovered emit picture in an amplified visual cryptography plan for which the figure size of the mystery pictures and the reproduced picture by stacking shares is the comparative concerning the first halftone emit picture. The resulting arrangement maintains the perfect security of the initially created visual cryptography approach. This methodology incorporates 2x2 piece substitution for creating shares from emit picture.

Keywords: cryptography, image processing, visual cryptography, secret sharing, Halftoning





































1. Introduction

Visual cryptography (VC), at first presented in 1994 by Naor & Shamir [1], is a secret digital image sharing method; this strategy is completely focused around black and white or binary pictures. Input information such as Images, is differentiated into shadows; by stacking these shadows it will reveal the original information with slightly degraded quality. These shadows uncover no data of the original image. Shares produced from input (secret) image may be circled to different parties, so that just by superimpose of a proper number of shares can uncover the input information, i.e. secret picture. Recovery of the secret information is conceivable done by stacking or superimposing the shadows and, therefore, the reconstruction strategy obliges no computation hardware or programming and could be fundamentally done by the human eye (human visual system). Visual cryptography secret sharing is one of most important issues in cryptography, can enable a secret, such as the cryptographic key, to be shared and protected among a group of participants. This is also used for security procurements subordinate upon biometrics [2]. Such as,

biometric information as facial, finger impression also signature pictures may be kept puzzle by allocating into shares, which could be appropriated for security to different parties. The secret information (image) can then be revealed, when all the parties gives their share pictures for superimposition.

So far many scientists have done lots of research in the field of extended visual cryptography. For example: there are some multiple secret information sharing scheme. In addition some of them have improved their algorithm to safe their secret information from intruder. Moreover, due to the advancement in computer era, it facilitates the development of electronic devices such as digital cameras, digital images have been widely used in many area. Consequently, the secret sharing methodology exposes the security problem relating to the protection of secret images such as military services, banking, and private images. Therefore, protecting image-based secrets becomes a critical issue in secret sharing.

Table 1: (2; 2) VC Scheme with 4 Subpixels

Secret pixel	□ (white pixel)						■ (black pixel)					
Pattern number	1	2	3	4	5	6	7	8	9	10	11	12
Shadow block 1	 [1010] [1010]	 [0101] [0101]	 [1100] [1100]	 [0011] [0011]	 [1001] [1001]	 [0110] [0110]	 [1010] [0101]	 [0101] [1010]	 [1100] [0011]	 [0011] [1100]	 [1001] [0110]	 [0110] [1001]
Shadow block 2	 [1010] [1010]	 [0101] [0101]	 [1100] [1100]	 [0011] [0011]	 [1001] [1001]	 [0110] [0110]	 [1010] [0101]	 [0101] [1010]	 [1100] [0011]	 [0011] [1100]	 [1001] [0110]	 [0110] [1001]
Decoded block	 [1010] [1010]	 [0101] [0101]	 [1100] [1100]	 [0011] [0011]	 [1001] [1001]	 [0110] [0110]	 [1010] [0101]	 [0101] [1010]	 [1100] [0011]	 [0011] [1100]	 [1001] [0110]	 [0110] [1001]

1.2 Review of Visual cryptography Schemes

The visual cryptography holds different plans these are -:

(A) **2 out-of 2 visual cryptography** interpret an ordinary plan of (2,2) VCS create 2 shares image from the original image and must superimpose both shares to produce unique original visual information. In general, two basic matrices are used to decompose the binary secret image into two shadows:

$$C(w) = \{[1\ 0\ 1\ 0; 1\ 0\ 1\ 0], [0\ 1\ 0\ 1; 0\ 1\ 0\ 1], [1\ 1\ 0\ 0; 1\ 1\ 0\ 0], [0\ 0\ 1\ 1; 0\ 0\ 1\ 1], [1\ 0\ 0\ 1; 1\ 0\ 0\ 1], [0\ 1\ 1\ 0; 0\ 1\ 1\ 0], \dots\} \quad (1)$$

$$C(b) = \{[1\ 0\ 1\ 0; 0\ 1\ 0\ 1], [0\ 1\ 0\ 1; 1\ 0\ 1\ 0], [1\ 1\ 0\ 0; 0\ 0\ 1\ 1], [0\ 0\ 1\ 1; 1\ 1\ 0\ 0], [1\ 0\ 0\ 1; 0\ 1\ 1\ 0], [0\ 1\ 1\ 0; 1\ 0\ 0\ 1], \dots\} \quad (2)$$

where the binary one(1) indicates a black pixel and the digit binary zero(0) indicates a white pixel.

According to table 1, In a given secret image if the pixel value is white, according to the followed algorithm it will randomly chooses one of the patterns from the matrix C_w to encrypt the pixel into its corresponding shadow blocks 1 and 2. On the contrary, if a given secret pixel is black, the encoder randomly selects one of the patterns from the matrix C_b to similarly produce the shadow blocks 1 and 2. Therefore, each secret pixel is transformed into two blocks consisting of 2 black and 2 white sub-pixels. After superimposing the shares the original image will be obtained [3].

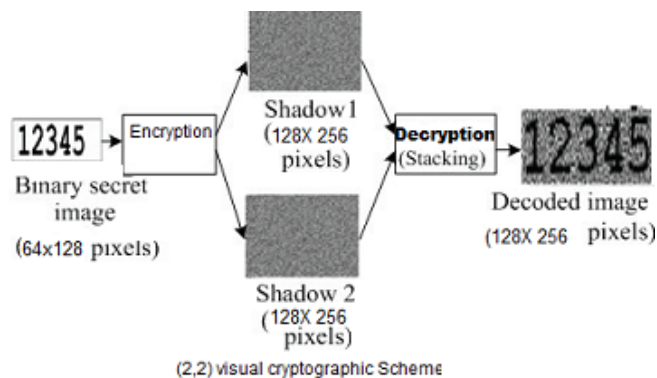


Figure 1: The 2-out-of-2 threshold Visual Secret Sharing

(B) **2 out-of n visual cryptography scheme** in this method of visual cryptography total n shadows will be generated from a secret image and any two of them is required to disclose the original information [4][5].thesis

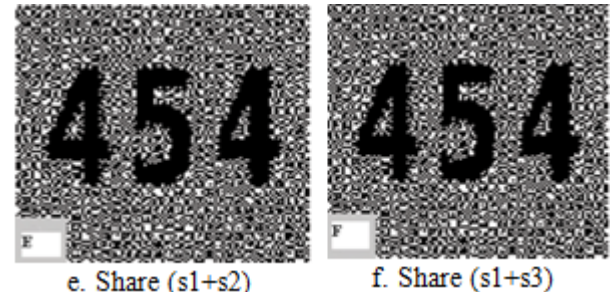
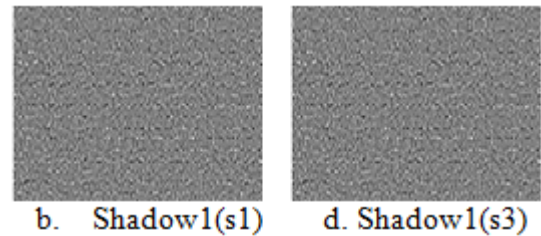
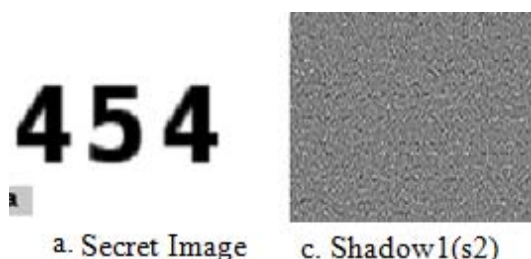
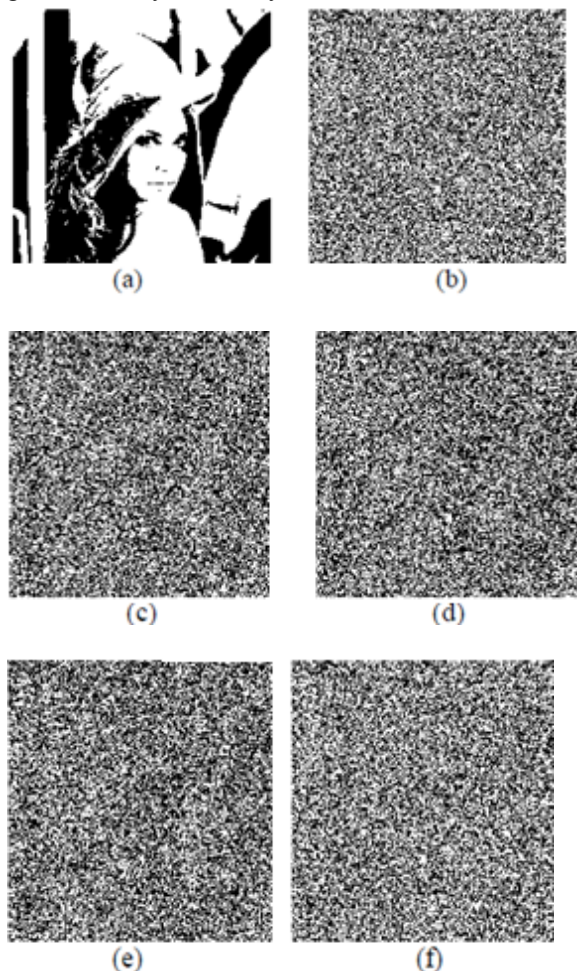


Figure 2: The 2-out-of-n VCS using the image SI1 (a) SI1 (b) S1, (c) S2, (d) S3, (e) S1+S2, (f) S1+S3

In this scheme any two out of any n shares are capable to restore original information as shown above. The quality of picture is also degraded. In addition the size of recovered image gets expanded.

(C) **K out-of N visual cryptography plan (k, n)** Visual Cryptography Scheme In past plan of (2, 2) visual cryptography, both the shares are required to acquire to uncover secret picture. In the event that one of them impart gets hacked by somebody or lost,



Secret information can't be uncovered and is an imprisonment of keeping all the shares secure to uncover shadow image and parties can't stand to lose a single offer. To beat this issue and provide for some adaptability in this plan, base model of visual cryptography introduced by Naor and Shamir could be summed up into a visual variation of k out of n visual cryptography plan [6]. In (k, n) visual cryptography plan, n shares produced from input information (secret picture) and circulated to all the parties. To extract the original information, we need just k shares, when all k shares are superimposed together, (where k lies between 2 to n), we can get secret image. If retriever has any of $(k-1)$ or less share, the information can't be uncovered. It provides for some attainability to client. On the off chance that gathering lost one or two of the shares still secret picture could be acquired, if least k *number of shares is gotten*.

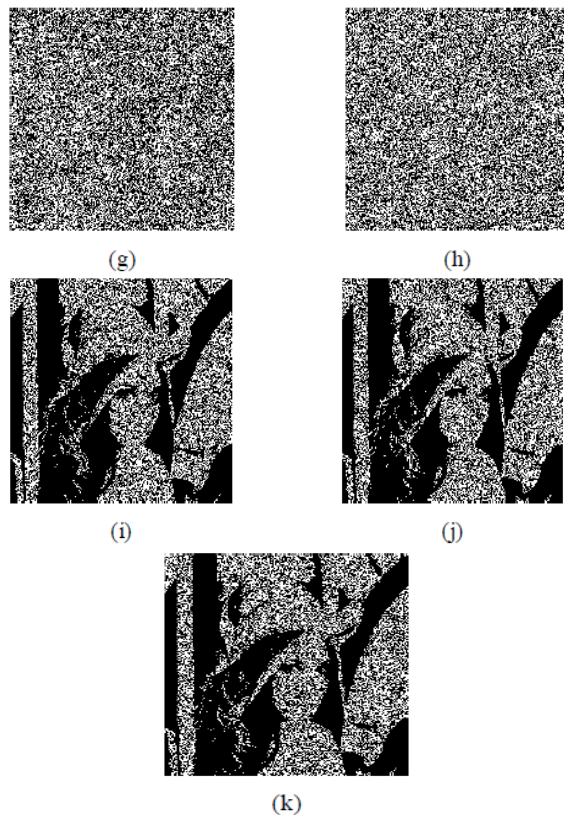


Figure 3: The 3-out-of-6 VCS with ABM of SI2: (a) SI2 (b) S1, (c) S2, (d) S3, (e) S4, (f) S5, (g) S6, (h) S3+S4, (i) S1+S2+S3, (j) S1+S2+S4, (k) S2+S3+S4

The $(2,2)$ extended visual cryptography plan presented [7] in this plan with the assistance of extension of one pixel in the mystery picture to 4 sub pixels which can then be decided to produce the obliged spread pictures for each one offer. It is completely secure and no offer picture releases any secret data of the first picture. Figure 2 shows a $(2, 2)$ plan holding the first binary secret picture.

Generally visual cryptography performs on binary visual information (Images); it can additionally be performed on gray scale images by changing them in halftoned images by using Halftoning algorithm. So halftoning is methodology of changing gray scale image into black and white picture into parallel picture this procedure stated as preprocessing

venture for visual cryptography. Then again, the procedure of halftoning connected to a grayscale picture realizes a reduction of the picture quality and since visual cryptography plots in like manner realize a diminishment in picture quality, mitigating picture defilement transforms into a key objective in a visual cryptography plan. Past plans coordinating halftoning and visual cryptography have encountered issues, for example, size expansion of output image (that is, obliging basically more pixels for the shares and/or delighted discharge picture) [8] and exchange off of the security of the plan [9].

The objective of the exploration outlined in this paper is:

1. To create a safe (k, n) visual cryptography plan, which do not need any computation and decryption methodology.
2. Generated shares or shadow must be meaningful, i.e. some stego image is used to cover the shadows, so information can't be pretended as secret information.
3. After stacking all shadows together there must not be any pixel expansion.
4. The proposed scheme is capable of restoring secret images with different resolutions by stacking different quantities of shadows together.
5. It can support all formats of image as input visual information.

2. Block Replacement Process on Halftone Image (Pre Processing Scheme)

Around there, we contemplate the order of visual cryptography to grayscale scale pictures by first changing over the pictures to a parallel picture by applying a halftoning plan. In the wake of making a halftone picture, to secure the picture size when applying visual cryptography and extended visual cryptography, clear plan may be connected. For example, a basic, secure plan that is not hard to execute is focused around a piece savvy technique to preprocessing the parallel halftone picture before applying visual cryptography [8]. In this paper we incorporate some typical methodology of piece substitution these are-

(A) Simple block replacement according to this scheme, it consider The SBR plan recognizes group of four pixels from the halftone secrete picture in one 2×2 blocks, alluded as a secrete block or square, what's more creates the shares block by block (instead of pixel by pixel). As every secrete block with four pixels encodes into n secrete shares each one holding four pixels, the size of the reveled picture is the same as the first secrete picture after stacking the any k shares among n shares together. In this method, all the secrete blocks in a picture need to be transformed before visual cryptography encoding and every secrete block is swapped by the comparing foreordained applicant, which is a block containing 4 white pixels (a white block) or a block containing 4 black pixels (a dark piece). The SBR preprocessing method is particular based upon various dark and white pixels in every secrete block. On the off chance that the amount of black pixels in a secrete block is bigger than or equivalent to 2, the secrete block replace by a black block. On the off chance that the amount of black pixels in a secrete block is short of what or equivalent to 1, it is

changed over to a white block. This step produce a new secrete picture which holds just white and black blocks. The picture got from this step is alluded to as a processed secret image. The prepared picture is ready to utilized as a secrete picture with in visual cryptography methods, for example, traditional VC or EVC. A problem is associate with this scheme is if block contain exactly two black pixel and two white pixel. To remove this problem a new scheme was introduced called balanced block replacement (BBR) method.

(B) **Balanced Block Replacement (BBR)** the novel perspective in this procedure is to perform the square substitution such that there is a predominant leveling of white and dull in the transformed emit picture. The beforehand SBR system achieves darker pictures, since piece which hold two white and two dark pixels are changed over to a dark pixel. In the BBR approach, it adjusts white and dark in the handled picture by giving some applicant squares to dark and others to white. The work of these competitor pieces perform arbitrarily this enhances the nature of visual prepared emit picture [8].

3. Proposed Algorithm

For the objective proposed in this paper, to achieve this, a friendly progressive visual secret sharing is used. The proposed offering plan applies a 2×2 -sized, square block operation to investigate the block relationship between the secret block in the secret image and the stego block in the stego image and to create the corresponding shadow block as indicated by the block relationship. A flowchart that demonstrates the proposed offering technique is displayed in Fig. 4. In this, let the halftone secret picture and the halftone stego picture be meant as STE and STG, individually. What's more, let the two pictures STE and STG have the same size, i.e., $row1 \times col1$. Likewise, for consensus, let the picture STE be part into n shadows (i.e., STE1, STE 2, ..., STE n) for n members. The general method is definite as below in pictorial form:

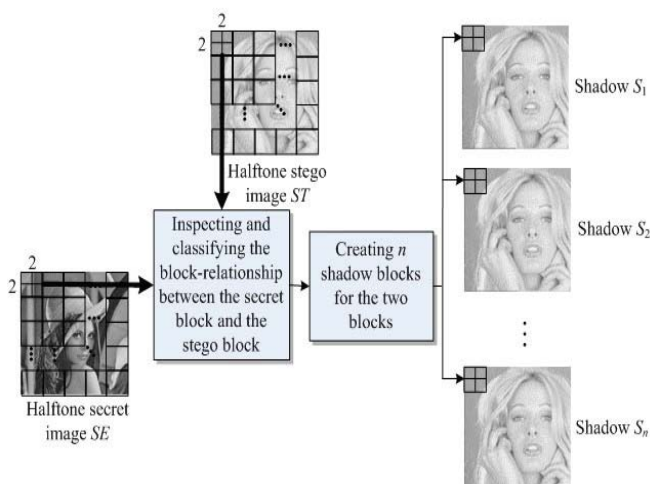


Figure 4: Block diagram of proposed scheme

Step1. To start with believer, read the input visual information (image) from any location from your working desk, and check whether secret information is RGB image or gray scale picture, if it found RGB image convert it into

halftone picture as we are working on halftoned image. Before halftoning of an gray scale picture the measure of a picture ought to be altered to evading pixel extension. For halftoning Jarvis Juides halftoning calculation is utilization. This picture is alluded as " halftoned secret picture"

Step2. Thus an alternate picture is taken to hide the secret picture by this picture. Again first step is petitioned this picture likewise. This picture is alluded as " stego picture".

Step3. To conceal the discharge picture by hide it from a stego picture. To improve the security reasons, logical bit anding operation is perform between these two images (haltioned Stego Image & halftoned secret Image) This new picture alluded as "combined picture" denoted as "bcomb".

Step4. Now start working towards share creation, To begin with, the image STE is fractioned into a number of non-overlapping secret blocks, size of each block is 2×2 . In addition, the image STE is similarly fractioned into 'n' non-overlapping stego blocks to maintain the 2×2 pixel relation. Now, the p th secret block, for $1 \leq p \leq (row_1 \times col_1)$, is compared with the p th stego block to obtain their block relationship. In the proposed scheme, there are three types of the block relationships. Here, continuing to maintain the originality, assume that the p th secret block is denoted as: $Bsec_j = \{bsec_j | 1 \leq j \leq 4\}$ and the p th stego block is symbolized by $Bstg_j = \{bstg_j | 1 \leq j \leq 4\}$. To obtain the type of the block relationship between $Bsec_i$ and $Bstg_i$, a compared block $Bcomb_j$ denoted as

$Bcomb_i = \{bcomb_j | 1 \leq j \leq 4\}$, is first generated by executing the logical operation "AND" on the two blocks as formulated as

$$ScBsec \& Bstg_{ii} =, \text{ for } 1 \leq j \leq 4 \quad (3)$$

$$Bcbsec \& bstg_{ii} =, \text{ for } 1 \leq j \leq 4 \quad (4)$$

where "&" means the "AND" logical operation.

Now, as per the developed algorithm in MATLAB the proposed scheme counts the total numbers of black pixels in the bitanded block, $Bcomb_i$ to classify the block relationship between secret block $Bsec_i$ and stego block $Bstg_i$ into one of three types:

- 1) If the total count of black pixels in the bitanded combined block $Bcomb_i$ is more than or equal to 2, the block relationship of the two blocks $Bsec_i$ and $Bstg_i$ corresponds to the designed function named Type-1.
- 2) If there is only one black pixel in the compared block $Bcomb_j$, the block relationship of the two blocks $Bsec_i$ and $Bstg_i$ corresponds to the designed function Type-2.
- 3) If there are no black pixels in the compared block $Bcomb_j$, the block relationship of the two blocks $Bsec_i$ and $Bstg_i$ belongs to the group named Type-3.

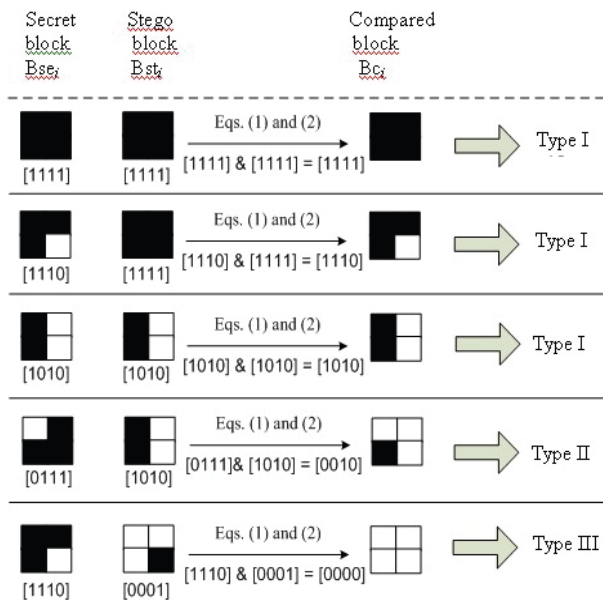


Figure5: Block relation between STE & STG

4. General Algorithm Description

In this scheme of visual cryptography it includes the various algorithms for halftoning, shares generation. This section describes some general information related to the algorithm. These are:

Proposed Algorithm:

Type 1 algorithm basically elaborate the block relationship between two (STE and STG). More generally, the block relationship of Type I means that the two blocks are the most similar to each other. This algorithm is describes the relation between STE & STG by counting the total black pixels in combined bitanded image. If all pixels in the Bcomb are black or greater than two, we just convert those blocks in base matrix, on random basis we can select any one of the matrix below mentioned.

$b01=[1,1;0,0]$, $b02=[0,1;1,0]$, $b03=[0,0;1,1]$
 $b04=[1,0;1,0]$, $b05=[0,1;0,1]$, $b06=[1,0;0,1]$

The same process will be repeated for n times, where n is the total number of shares. Here 1 stands for black and 0 stands for white.

In (k,n) scheme n zero matrix of (size of shares equal to the size of processed image) is requires for share generation. In each iteration 2x2 block of a single zero matrix is replace by selected base matrix.

Whereas the relationship of STE and STG block, Type III indicates that the two blocks are most unmatched to one another.

TYPE-2: If the values in block depict the relationship between the two blocks Bse and Bstgi belongs to Type-2, then shadow creation will take steps. In the first step,

1. When count of ones in Bcombi (compared block) is only one, we take the comparison loop for bse and check for the position of ones in the corresponding block, and simultaneously take a 2X2 blank matrix of zeros and replace any one of them by one as per by the Bcombi. Output of this algorithm is illustrated shd.

2. In final step, a quality factor, which can be depicted as $Qtf = 1/qt$ with $0 < qt \leq 1$, is come into the picture in proposed methodology to decide whether or not another one is randomly select from the secret extracted block Bse as another corresponding one in the shadow block. Here, when Qtf (quality factor) is equal to 1, the proposed methodology executes the 2X2 block as made above. Note the important point, that pixel value to be selected randomly from the Bse(secret block) must be placed at the position different from the position of the one's in the Bcomb(compared block). Consequently, each shadow block also comprises two 0's and two 1's. Because the proposed methodology chooses another 1's at random from the Bse (secret block) to construct a shadow block during the sharing procedure, the data of the secret block may be totally uncovered when more shadow blocks are stacked together. Conversely, when Qtf is less than 1, not every shadow block needs to do such a choice for development. All the more decisively, for each one shadow blocks, the likelihood that another dark pixel is looked over the secret block Bse to be an alternate relating dark pixel in the shadow lock is $1/qt$. It is evident that some shadow locks can have a slight degradation of image quality on the grounds that the stego blocks is not completely decimated.

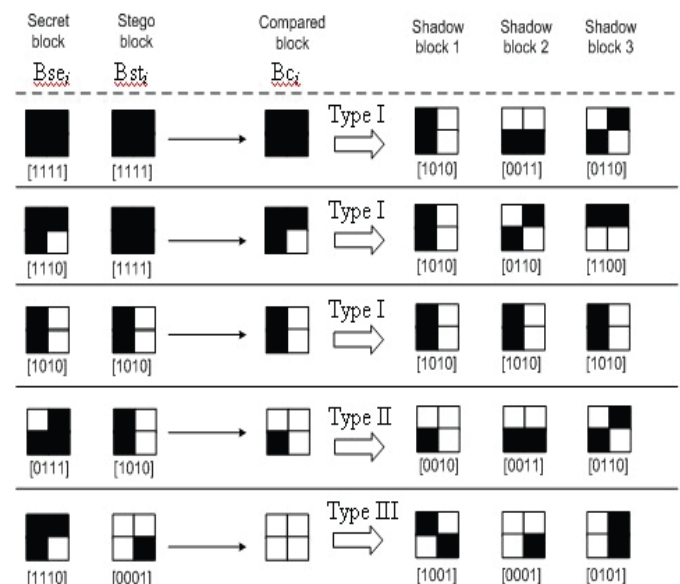


Figure 6: Interpretation of generating 3 shadow blocks from two blocks Bse and Bste.

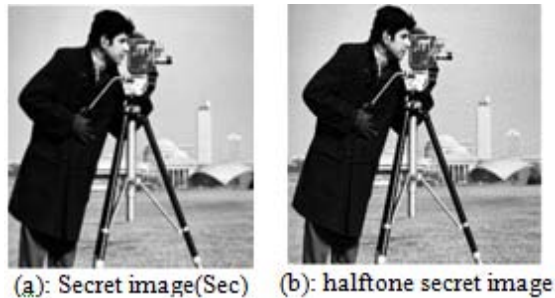
TYPE-3: If the values in block depict the relationship between the two blocks Bse and Bstgi belongs to Type-3, then shadow creation will take 2 steps. In the first step,

1. When count of ones in Bcombi (compared block) is zero, we take the comparison loop for bse and check for the position of ones in the corresponding block, and simultaneously take a 2X2 blank matrix of zeros and replace any one of them by one as per by the Bcombi. Output of this algorithm is illustrated shd.
2. In the final step, we introduce the concept of quality factor (Qtf), on the basis of Qtf, we decide that whether we can select another black pixel(1's) from extracted stego block(Bstgi) or not, to transfer it in blank matrix(zeros matrix). Figure 6 represent model for the

creation of the shadow blocks, where the number of shadows is set to 3 (i.e., $\text{ind} = 3$), and Q_{tf} is set to $1/2$. Output of this algorithm is illustrated st. Finally again perform bitor operation in between shd and st and save the result in shd.

After execution of all three algorithms, finally stack the total shares from all parties to uncover the original secret visual information (image)

5. Results Image



(a): Secret image(Sec) (b): halftone secret image



(c): Negative of halftone secret image



(d): halftone cover image



(e): (24, 24) share generation



(f): Reconstructed Image after stacking with $Q_{tf}=1$;

Figure 6: process of (k, n) visual cryptography scheme

6. Conclusion

In this paper, we have accomplished our proposed objective and created visual cryptography without pixel extension with genuine meaningful shares. We have showed that using best pre-processing steps of halftone pictures based upon the parts of the first secret image, we can deal with incredible quality image shares and the got mage. Note that distinctive procurement's can in like manner benefit from the pre-processing strategy, for instance, diverse picture visual cryptography, which hides diverse images in shares [11].

References

- [1] M. Naor and A. Shamir, "Visual cryptography", in EUROCRYPT'94 Proceedings, Lecture Notes in Computer Science, Springer-Verlag, vol. 950, pp. 1-12, 1995.
- [2] A. Ross and A. A. Othman, "Visual Cryptography for Biometric Privacy", IEEE Transactions on Information Forensics and Security, vol. 6, no. 1, pp. 70-81, 2011.
- [3] N. Askari, C. Moloney and H.M. Heys, "A Novel Visual Secret Sharing Scheme Without Image Size Expansion", IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), Montreal, pp. 1-4, 2012.
- [4] Doug Stinson, *Visual cryptography and threshold schemes*, Dr. Dobb's Journal, pp. 36-43, April 1998.
- [5] Borko Furht, Edin Muharemagic and Daniel Socek, *Visual and Audio Secret Sharing*, Multimedia Encryption and Watermarking, Springer, pp.163-192, 2005.
- [6] Moni Naor and Adi Shamir, "Visual cryptography". In Proceedings of Advances in Cryptology, EUROCRYPT 94, Lecture Notes in Computer Science, 1995, (950):pp. 1-12.
- [7] G. Ateniese, C. Blundo, A. De Santis and D.R. Stinson, "Extended Capabilities for Visual Cryptography", Theoretical Computer Science, vol. 250, pp. 143-161, 2001.
- [8] Z. Zhou, G.R. Arce, and G. Di Crescenzo, "Halftone Visual Cryptography", IEEE Transactions on Image Processing, vol. 15, no. 8, pp. 2441-2451, 2006.
- [9] M. Nakajima and Y. Yamaguchi, "Extended Visual Cryptography for Natural Images, in Proceedings of WSCG", pp. 303-310, 2002.
- [10] N. Askari, H.M. Heys, and C.R. Moloney, "An Extended Visual Cryptography Scheme without Pixel Expansion for Halftone Images" IEEE Canadian Conference of Electrical and Computer Engineering (CCECE) E vol. 6, no. 1, pp 33-38, 2013.
- [11] C.C. Wu and L.H. Chen, "A Study on Visual Cryptography", Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, 1998