Visual Cryptography Using Half-toned Images

P. J. Padalkar, S. S. Kumar, J. Albert, I. Menezes
Department of Information Technology, Don Bosco Institute of Technology, Mumbai, India.
pprasadj@dbit.in

Abstract: **With an exponentially increasing pile of information dumped across the World Wide Web, securing private and public information has never been more imperative. Over the years, encryption techniques have evolved to include many steps with multiple calculations (performed iteratively) to help avoid revealing the concealed message within. These come with their inverse counterparts which unscramble the code to reveal the message, and includes (almost or maybe even more) steps with corresponding inverse calculations (again performed iteratively). Thus, it is only fair to say that both, encryption and decryption, when coupled together; are not only time-consuming but resource-consuming too. When included in an application, it would add to the net time taken and create a strain on the resources. Visual Cryptography provides an effective solution to solve this with fewer steps and lesser complexity. Its major computations are focused on encrypting the image while a simple operation deciphers it. The key process involves application of the twisted secret sharing to the image.**

Keywords: encryption, twisted secret sharing scheme.

I. INTRODUCTION

Visual Cryptography (VC), as the name suggests, adds a visual dimension to the whole security workspace. It encrypts visual information. It thus works on informative images, encrypts it, to what appears as a series of randomized pixels and decrypts it using a simple XOR operation. This greatly reduces the total time and cost spent in developing and maintaining information security.

In order to hide a message, VC never includes substitution of any character with an encrypted character. Though in terms of defining it, we said, it encrypts only visual information; this can be extended to suit all types. That is, any information whether a set of bits, characters, numeric or a combination of these, could be first visually produced as an image before being subjected to VC. This image is then encrypted by the action of the algorithms to deceive the perpetrator and secure the message.

An important application of VC is its use in digital watermarking to authenticate the originality of a document. This includes embedding of the private secret document with a copyright share, which won't be visible to the naked eye. But, overlapping it with its corresponding share reveals the copyright information, and thus, the authenticity of the document.

VC can be used to protect biometric templates in which the decryption doesn't require any complex computations [1]. Other applications include Remote Electronic Voting, Anti-Spam Bot Safeguard, Banking Customer Identification, Message Concealment and Key Management.

II. LITERATURE SURVEY

A. Halftone Visual Cryptography

In Visual cryptography, a secret binary image is encoded into shares of random binary patterns. If the shares are printed onto transparent or translucent sheets, then the encrypted image can be reproduced and can be seen by physically combining or overlapping proper shares. Half-toning is a method of converting high bit pixels to into printable lower bit format. The half-toned image is generated by the method of blue noise half-toning, or pixel reversal. The technique underlying the two-out-of-two halftone visual threshold scheme is extended to cryptography, where a secret binary image (secret image) is hidden into halftone shares. [2]

B. Secret Sharing Schemes for Protection of Digital Images

This paper focuses on the major algorithms of secret image sharing schemes. It first describes a secret sharing scheme based on polynomial interpolation. This technique creates a (k-1) degree polynomial function to compute shares using the secret image, where k is the minimum number of shares required to obtain the secret image. It also describes a (r, n) scheme where, the original image can be obtained if at least r or more of n *shares* are obtained; however $r - 1$ shares cannot be used to obtain the original image. It uses the polynomial function and all k coefficients of the polynomial to share the secret pixels so that the size of the image shares is reduced to $1/k^{th}$ of the secret image [3]. It then requires k or more image shares to reconstruct the secret image. The drawback of this scheme is that the original image cannot be recovered completely. Another secret sharing technique was proposed where a secret image with a pixel value greater than 250 is divided into two but though this technique completely recovers the image it

produces expandable shares. Visual Secret Sharing (VSS) is another scheme based on the *(k, n)* threshold concept but it suffers from two drawbacks: Pixel expansion and Low image quality.

C. An Extended Visual Cryptography Scheme without Pixel Expansion for Half-toned Images

In the basic (2, 2) scheme for visual cryptography, the resulting shares and the recovered image contains four times more pixels than the actual image. This is resolved by using a block-wise approach to dividing the pixels. There are two algorithms suggested for this purpose: The Simple Block Replacement (SBR) Algorithm and the Balanced Block Replacement (BBR) Algorithm [4]. Results of both reveal that the SBR produces darker images compared to BBR, which produces images that bear more resemblance to the actual image.

D. A Comparatively Study on Visual Cryptography

VC has been implemented with many variations based on number of secret images, pixel expansion, mode of deciphering [5]. This is summarized in TABLE I.

III. ALGORITHMS IMPLEMENTED

A number of algorithms with different techniques were searched and reviewed before finally implementing the optimum ones for encryption. Some of them were modified indefinitely to suit our purpose. They are as follows:

A. Simple Block Replacement Technique

Simple Block Replacement (SBR) follows a block-wise concept. It first divides the image as shown in *Fig. 1.*, into 2x2 blocks each containing 4 pixels. Working one block at a time, SBR pre-processes the image, before the main process of producing image shares is initiated.

The algorithm is as follows:

1. Divide the image into a set of 2x2 blocks
2. BLOCK COUNT
   Count the number of black pixels in the 2x2 block
3. IF Count >= 2
   Convert all pixels in the block to BLACK
   ELSE
   Convert all pixels in the block to WHITE
4. Perform steps 2. & 3. iteratively for all blocks within the image.

B. Balanced Block Replacement Technique

Balanced Block Replacement (BBR), unlike SBR, follows a cluster-wise concept. It first divides the image as shown in *Fig. 2.*, into 4x4 clusters each containing 16 pixels. Each cluster is then sub-divided into four 2x2 blocks each containing 4 pixels. BBR then works, one cluster at a time, pre-processing the image, before the image shares could be produced.

In comparison to SBR, there's just one operation BBR performs differently. That is, if the black pixel count for a block has been found equal to 2, then it performs a check to see that if on converting the block completely to black/white, how it would vary with respect to the black pixel count of the cluster.

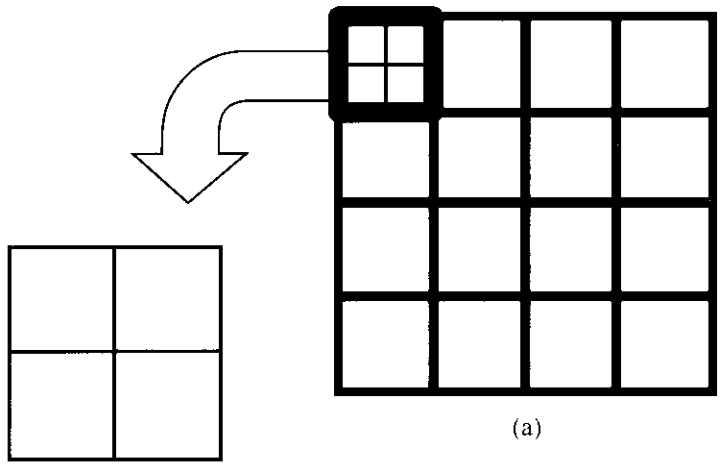


Fig. 1. Block Position with respect to the Image
(a) Image divided into set of 2x2 blocks
(b) 2x2 Block showing group of 4 pixels

The algorithm is as follows:

1. Divide the image into a set of 4x4 clusters

Fig. 1. Block Position with respect to the Image
(a) Image divided into set of 2x2 blocks
(b) 2x2 Block showing group of 4 pixels

2. PRE-CONVERSION COUNT
   Count the number of black pixels in the 4x4 cluster and save it as 'old'.
3.
3.1. Divide the cluster into a set of 4 2x2 blocks numbering each from 0-3
3.2. BLOCK COUNT
   Count the number of black pixels in the 2x2 block
3.3. IF count > 2
   Convert all pixels in the block to BLACK
   ELSE IF count < 2
   Convert all pixels in the block to WHITE
   ELSE
   Flag [*block_number*] = true
   where block_number = 0, 1, 2, 3
3.4. Perform steps 3.2. and 3.3. iteratively for all blocks within the cluster.
4. POST-CONVERSION COUNT
   Count the number of black pixels in the 4x4 cluster and save it as 'new'.
5. Perform 5.1. iterating i from 0-3

5.1. IF Flag[i] = true
THEN perform 5.1.1.

5.1.1. IF ([difference between(old, new+2)] < [difference between(old, new-2)])
Convert all pixels in the flagged block to BLACK
ELSE
Convert all pixels in the flagged block to WHITE

6. Perform Steps 2-5 for all clusters within the image

TABLE. I: Comparisons of Different VC Techniques

Technique	Number of Secret Images	Pixel Expansion	Merit	Demerits
Traditional VC	1	1:2	Provides security for binary images	Does not generate meaningful image shares
Extended VC	1	1:2	Generates meaningful share	Contrast loss occurs
Random Grid VC	1	1:1	No pixel expansion	Lower visual quality
Multiple Secret Sharing VC (Version 1)	2	1:4	Image encrypts two secret images between two shares. Rotating angle is 90 degrees.	Size of the shares is 4 times the size of the main secret image.
Progressive VC	1	1:1	No pixel expansion.	No absolute guarantee on the correct reconstruction of the original pixel.
Multiple Secret Sharing VC (Version 2)	2	1:4	Rotating angle varies.	Pixel expansion is more.
Halftone VC	1	1:4	Provides meaningful share images.	Trade-off between pixel expansion and contrast of original image.

G. Secret Sharing Concept

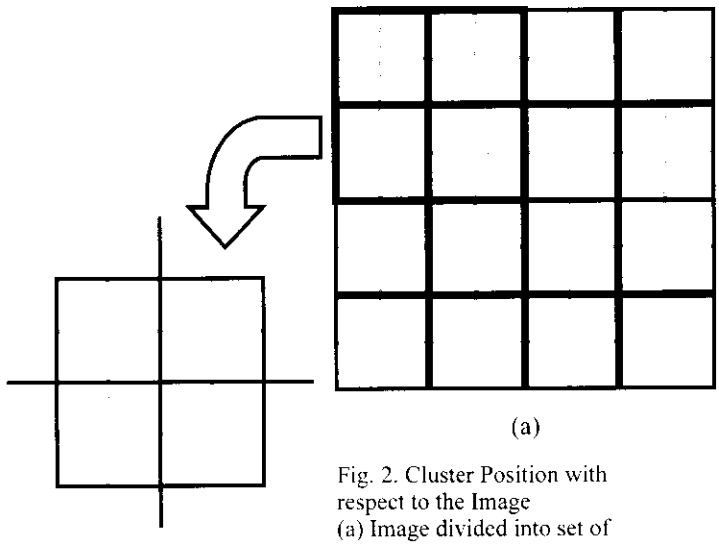
The secret sharing concept determines how many parts (shares) the secret image would be split into and how many of them would be required to reveal the secret image. Depending on the type of scheme implemented, the block representation pattern in the shares would change accordingly.

1) The (2, 2) Scheme

The (2, 2) scheme splits the secret image into 2 shares with both of them being required to reveal the same.
After an image has been pre-processed with SBR/BBR, the image contains only 2x2 blocks of white and black pixels. It is now ready to be split across the two shares. Based on the color of the pixels in the block, the pixels in the two secret shares are determined randomly as shown in *Fig. 3.*

2) The (2, 3) Scheme

The (2, 3) scheme splits the secret image into 3 shares and any two of them are superimposed to reveal the same. The



(a)

(b)

Fig. 2. Cluster Position with respect to the Image
(a) Image divided into set of 4x4 clusters
(b) 4x4 Cluster split into four 2x2 blocks

output slightly differs from that of (2, 2) scheme. The white block pixels, like the above, retain 50% of its white colour. But, the black block pixels aren't always 100% black. There is a 1/6 chance that it will be completely black. In the rest of the cases, it's always 75% black i.e. out of the four black pixels in the black block; after superimposing the two shares only 3 pixels would be black and the remaining one would be white. Thus, this scheme won't be as efficient as (2, 2).

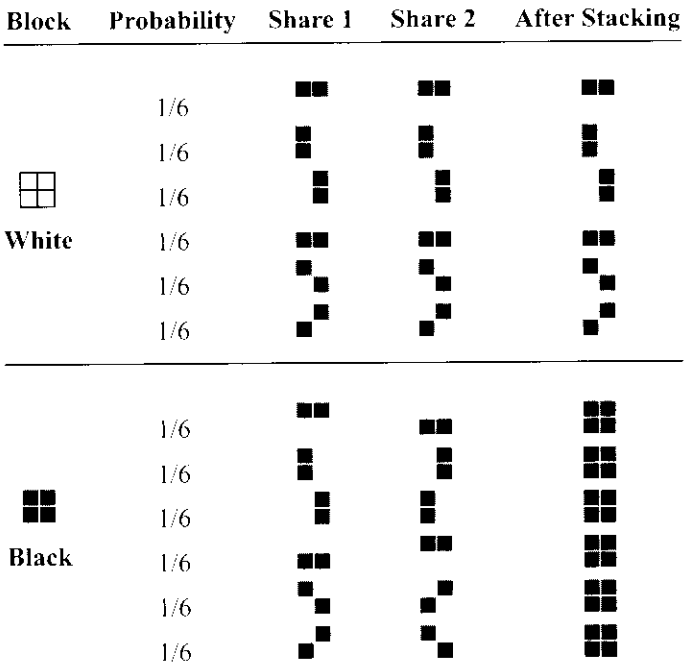


Fig. 3. Pattern showing Block representation used in the two shares of the (2, 2) scheme

D. Modification to the algorithm

1) BBR with Overlapping Clusters

Though BBR was proposed as an improvement to SBR and while it does improve the picture clarity, BBR was modified to suit overlapping clusters such that when clusters are iterated, two blocks from the previous cluster are retained with their modified pixel values.

An example is shown in *Fig. 4.* The step-by-step processing of this is shown in *Fig. 5.* This renewed technique has been experimented to give clearer images with even smoother edges.

2) Use of Block over Pixel in Sharing Schemes

The secret sharing methods supposedly worked on secret images directly. Due to this, the image shares suffered a pixel expansion of about 1:4. This increased the size of the shares four-fold. That is, a 1024x1024 secret image would produce shares with dimensions 4092x4092. This was a major drawback.

Therefore, instead of processing the image pixel-wise, we first divide the image into blocks and traverse the image based on a block-wise approach.

Pre-processing the image with SBR/BBR very conveniently eliminates pixel expansion. Having processed the image with one of the two, the output image would throughout contain only 2x2 blocks of pixels which are either completely black or white. Producing shares from this image doesn't require unnecessary redundancy of pixels introduced by earlier techniques.

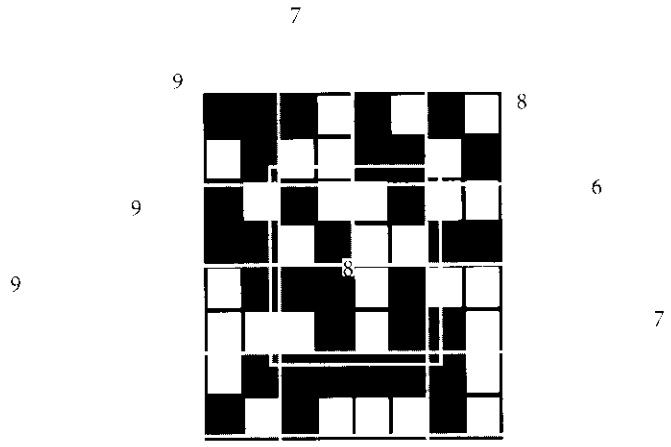
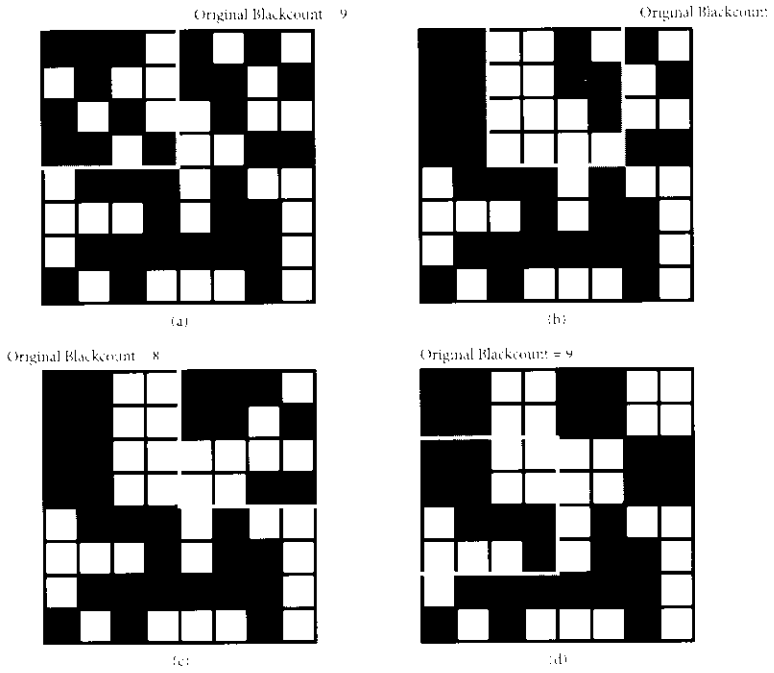


Fig. 4. A representation image showcasing the Overlapping Clusters with Initial Number of Black Pixels in each cluster



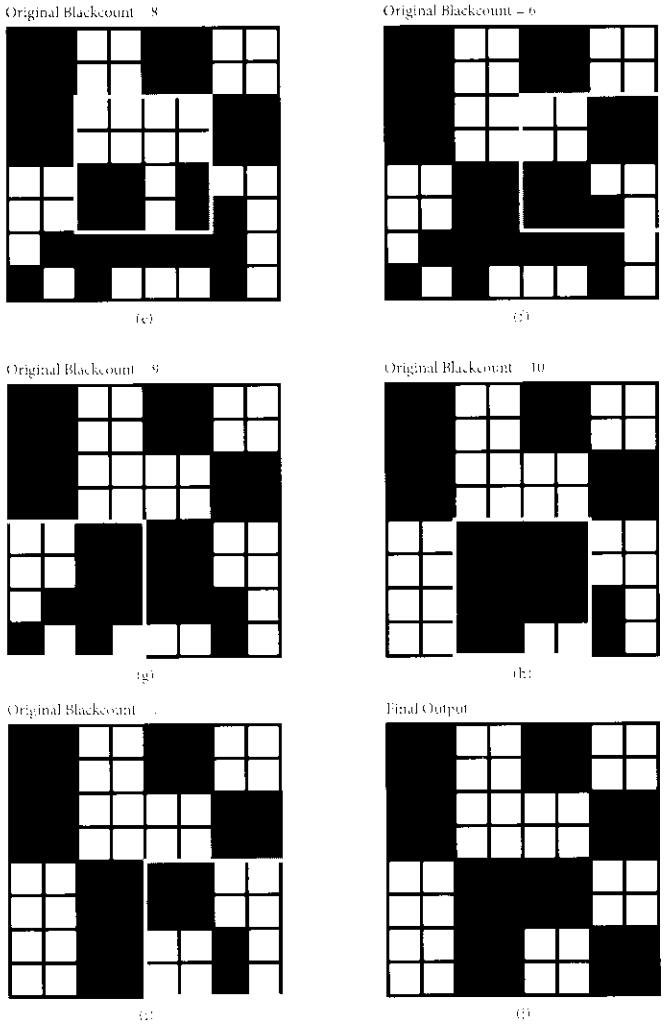


Fig. 5. A representation image showcasing the Overlapping Clusters with Initial Number of Black Pixels in each cluster

IV. RESULTS

In all, 6 codes were developed to achieve the desired security in Visual Cryptography. Three of their outputs are shown in *Fig. 6.* All *(b), (c)* and *(d)* are outputs obtained from the Original Image.

Due to the inability to develop a half-toning algorithm, these codes were experimented on readily available half-toned images and other binary images. Half-toning was used to convert grey-scaled images into a series of black dots of varying shapes and sizes. This made the image binary in black and white, but still giving the effect of different shades of grey.

Also, these images were taken in their bitmap format and a standard dimension of 256x256.

The first output obtained on implementing the (2, 2) scheme wasn't satisfactory. As it can be seen in *Fig. 7.*, the boundary of the image can be easily made out in the second share and nullifies the whole idea of keeping the image secure. Later, the reason for this was found out to be the usage of only one standard pattern out of the six available for black and white blocks. (*Refer Fig. 3.*). Also, for all images that were experimented upon, all produced the same standard first share. Thus, the first share of any image could be used with the second of another to reveal the secret image. This greatly contradicts the entire purpose of Visual Cryptography.

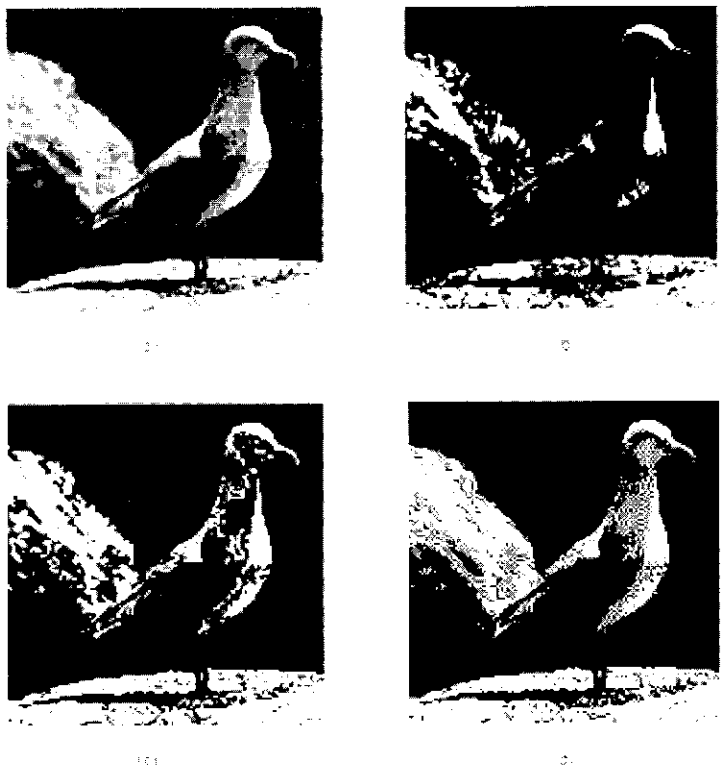


Fig.6. Processed Image Outputs
(a) Original Image
(b) SBR Output
(c) BBR Output
(d) BBR Overlap Output

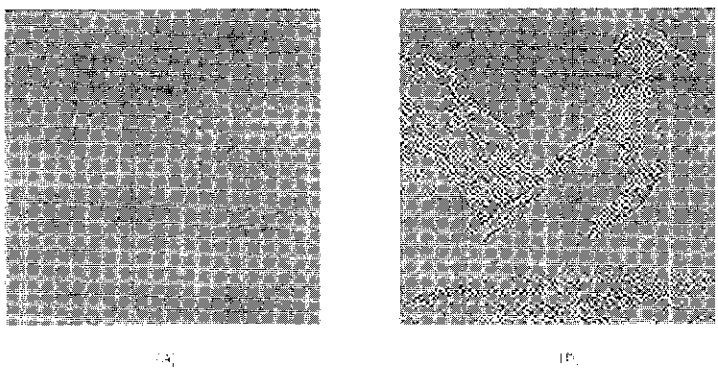
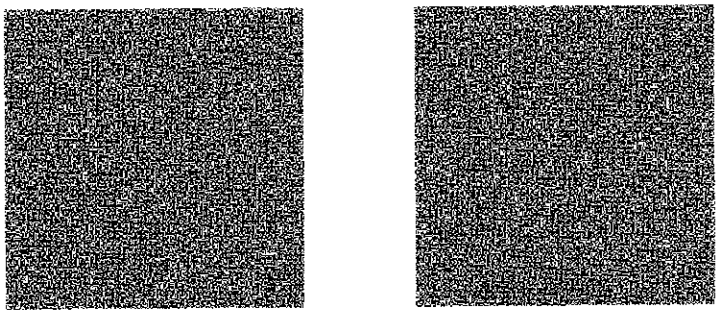


Fig. 7. Faulty (2, 2) Image Shares
(a) Standard 1st Share
(b) 2nd Share with visible boundaries

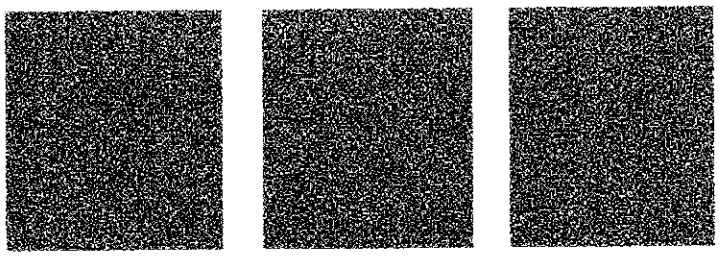
The code was later modified to include random selection from all 6 patterns for both white and black blocks. *(Again refer Fig. 3.).* Both (2, 2) and (2, 3) schemes were developed keeping this technique in mind and their outputs can be seen in Fig. 8. and Fig. 9.

The shares thus obtained contained random noise-like pixels which individually aren't able to reveal the image. These when stacked or overlapped produces the secret image.



(a) (b)

Fig. 8. Indistinguishable (2, 2) Image Shares
(a) 1st Share
(b) 2nd Share



(a) (b) (c)

Fig. 9. Indistinguishable (2, 3) Image Shares
(a) 1st Share
(b) 2nd Share
(c) 3rd Share

V. CONCLUSION

Visual Cryptography can thus secure any type of data - numbers, strings, images and bit alike; by producing them on an image and splitting it into shares. Compared to other techniques used, we could resolve the dispute involved with Pixel Expansion but the issue of Picture Contrast still remains for highly-detailed images being not all that clear. Also, for splitting the images into more than 3 shares, it includes the use of a 3rd or a higher degree polynomial which on researching continues to mention Pixel Expansion as a disadvantage. Using block replacement in these cases isn't feasible, as we would have to increase the block size from 2x2 to 3x3 and higher. Since, blocks behaves as the basic unit of the image, increasing the block size will only make the image more distorted with sharper edges and pixelated effects. Thus, to avoid pixel expansion and still get a well contrasted image from overlapping shares; (2, 2) Visual Cryptography Secret Sharing scheme is advisable.

REFERENCES

[1] Askari, Nazanin; Moloney, Cecilia; Heys, Howard M. (November 2011). "Application of visual cryptography to biometric authentication". NECEC 2011.

[2] Zhi Zhou, Member, IEEE, Gonzalo R. Arce, Fellow, IEEE and Giovanni Di Crescenzo, "Halftone visual cryptography," IEEE Transactions on Image Processing, Vol. 15, No. 8, August 2006.

[3] Amitava Nag, Sushanta Biswas, Debasree Sarkar and Partha Pratim Sarkar, "Secret sharing schemes for protection of digital images," CSI Communications October 2014.

[4] N. Askari, H.M. Heys, and C.R. Moloney, "An extended visual cryptography scheme without pixel expansion for halftone images," 2013

[5] Prashant B Swadas, Samip Patel, Dhruti Darji, "A comparatively study on visual cryptography," IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 pISSN: 2321-7308.