iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** I **Month of publication:** January 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A secured approach for sharing critical data on halftone image Using advance visual cryptography

Umesh A Jain[1], Vijendra S Somwanshi[2], Rutuja Y Ghule[3], Akshay R Butte[4], Mr.S.R. Lahane[5]
B.E Computer, Department of Computer Engineering, GES's R.H.Sapat College of Engineering, Nashik-422005, Maharashtra, India

Abstract: ***Visual cryptography is a secret sharing scheme which uses images divided as shares such that, when the shares are created, a hidden secret image is attached. In extended visual cryptography, the share images are developed that contain meaningful cover images. For processing halftone images that improves the quality of the share images and the recovered secret image in an extended visual cryptography scheme for which the size of the share images and the released image is the same as for the original halftone secret image. The remaining scheme maintains the perfect security of the original extended visual cryptography approach.***
Keyword: Visual cryptography, Pixel Expansion, halftone image, Share, Secret image.

I. INTRODUCTION

Visual cryptography is a secret sharing scheme, related on black and white images. Secret images are divided into share images it reveal no information of the original secret image. Shares may be given to various users so that only by collecting with an appropriate number of other users, can the resulting combined shares retrieve the secret image. Recovery of secret image can be done by imposing The share images and, hence, the decoding process Requires no special hardware or software and can be simple done by the human eye. The secret image can then recover when all users Release their share images which are then recombined. A basic 2 By 2 visual cryptography scheme produces 2 share images from an original image and must stack both shares to reproduce the original image. Generally algorithm produces n shares, but it only accept k shares to recover the secret image. To preserve the ratio for the recovered secret image for a 2 by 2 scheme each pixel in the original image can be replaced in the share images by a 2 * 2 block of sub pixels[5]. In the below fig 1, if the original pixel is white, one of six combinations 1 1 of share pixels is created. Similarly, the possible shares combination for black pixels is also shown. After collecting the shares with white transparent and black , the original secret image will be revealed. where white is equivalent to "0" and black is equivalent to "1" [6].

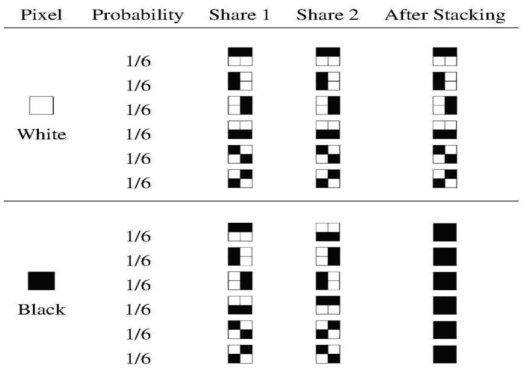


Fig 1 : Illustration of a(2;2) VC Scheme with 4 Subpixels

The recovered image has a low in visual Quality since a recovered white pixel is actually comprised of 2 white and 2 black sub pixels, while a black pixel is shown by 4 black sub pixels in the resultant image. The (2; 2) EVC scheme proposed in required expansion of one pixel in the original image to 4 sub pixels . which can then be selected to produce the required images for each share.

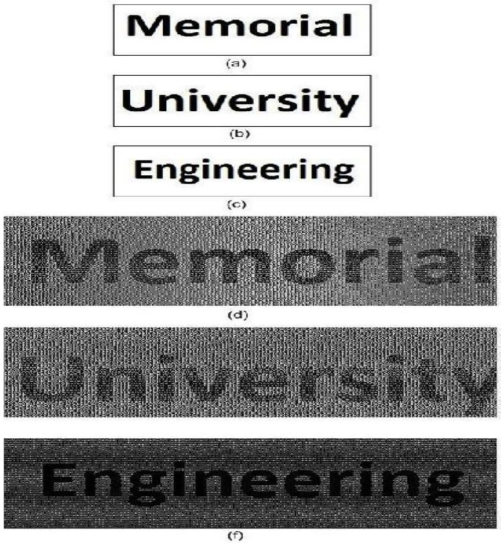


Fig 2 : Example of (2; 2) EVC Scheme: (a) first cover image;
(b) second cover image; (c) secret image; (d) share 1; (e) share 2; (f) recovered secret image.

First convert the gray scale image to a binary image[4]. Using half toning techniques to convert gray scale images to binary images is a useful pre-processing step for visual cryptography. The halftone process applied to a grayscale image results in a reduction of the image quality and since visual cryptography schemes also result in a reduction in image quality, Image degradation becomes an important objective in a visual cryptography scheme. Extended visual cryptography scheme, it does not require more pixels in the shares and recovered image than the original secret image and it also preserves a good quality image for both the shares and the recover image.

II. METHODS

A. Pre-Processing Halftone Images

The gray scale images by initially converting the images to a binary image using a half toning algorithm. After creating a halftone image, to maintain the image size when applying visual cryptography and extended visual cryptography method can be applied. a basic, secure method that is easy to implement is based on a block-wise strategy to per-processing the binary halftone image prior to applying visual cryptography[3]. Simple block replacement scheme is apply on groups of four pixels from the halftone secure image in one 2 _ 2 block, as a secret block, and produce the shares block by block than pixel by pixel. Each secret block with four pixels encodes into two secret shares each having four pixels, the size of the reconstructed image is the same as the original secret image. Secret blocks in an image need to be processed before visual cryptography encoding and each secret block is replaced by the corresponding pre assign candidate, which is a block with 4 white pixels or a block with 4 black pixels. The block replacement method in the SBR per-processing is based on a number of black and white pixels in every secret block. If the number of black pixels in a secret block is greater than or equal to 2, the secret block recovered to a black block. If the amount of black pixels in a secret block is small than or 1, it is converted to a white block color. The processed image used as a secret image in visual cryptography schemes such as regular VC or EVC. The SBR method is straight forward and is very clear for unprocessed binary secret images which have large number of all white and all black blocks. However, for halftone images, the distribution of black and white pixels within each secret block, in the images.

B. Improved Pre-Processing Scheme

The previously described SBR scheme results in high contrast images and blocks which contain two white and two black pixels are converted to a black block. Blocks of two white and two black pixels as assignment blocks. In the BBR approach, we balance white and black in the processed image by assigning some assignment blocks to black and others to white. The blocks are assignment randomly to black or white improves the visual quality of the processed secure image, even improved visual results can be achieved using an intelligent block replacement approach that considers as the characteristics of the original image in determining whether a assign block should be assigned to every black or white. The block replacement method proposed here tries to maintain the local ratio of black to white pixels in the processed image
close to the local ratio of black to white pixels in the original halftone secure image. Therefore, generated recovered image is

closer in quality to the original grayscale image.

C. BBR Method

The preparation of a grayscale image for use in visual cryptography involves 3 steps.

The first step is the transformation of a grayscale image into a halftone image and partitioning the halftone image into non-overlapping blocks of 2 _ 2 pixels. Then, the halftone image is divided into a number of overlapping squares of four 2 _ 2 blocks. Each grouping of 4 blocks is referred to as a set.

In the second step, the total number of dark pixels in each set from the halftone image are counted and saved in a template. This number is the point value for that set. The step then classifies all the secret blocks containing 1 black (resp. white) pixel. If the secret block contains 1 black (resp. white) pixel, it is converted to a white (resp. black) block. The image obtained from this step is referred to as the initial processed image.

The third step begin from the first initial block in the top left of the first cluster of the initial processed image. The processing of the blocks in each set starts from the top left piece, then change from left to right and top to bottom in raster format. When the first candidate block in a cluster is identified, the numbers of dark pixels in the set are counted.

The idea is to keep the number of dark and white pixels in each set of the initial processed image as close as possible to the corresponding point value from the set of the real halftone picture. Therefore the number of dark pixels in the case of changing the contender piece to a dark or white block is computed and is compared to the point value that was derived for the same set in the real halftone picture. If the corresponding contender block converts to a dark block, 2 pixels will be added to the number of black pixels in a set and if the contender block turns to white block, 2 dark pixels will be deducted from a set. The change is based on the smallest difference between the threshold and the number of black pixels in the image being processed. If changing the contender piece to black makes this difference smaller, the contender piece is changed to a black piece. Similarly, if turning the contender block to white makes this difference smaller, the block converts to a white piece. In the case that turning the candidate to dark or white produces the same difference, the piece randomly changed to either a black or white piece.

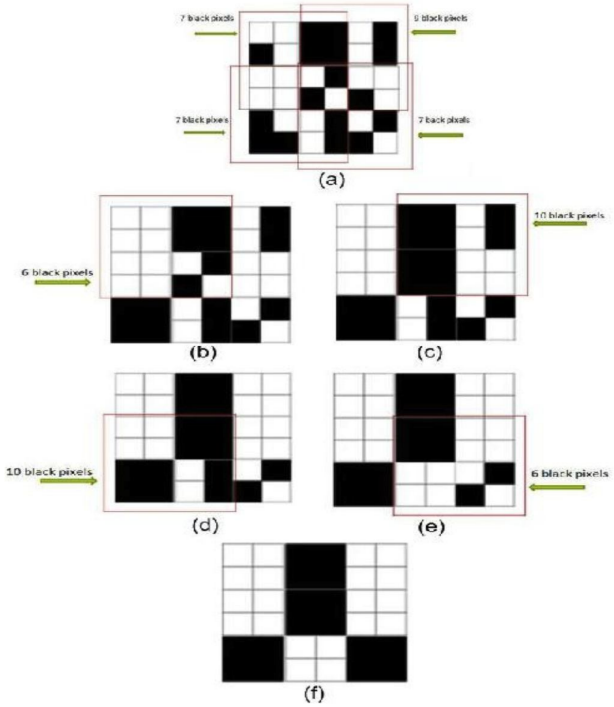


Fig 3 : Example of the BBR Method

III. SYSTEM

A. Encoding Algorithm

For a given value of, the transparencies can be continuously generated with the (t,∞) OptPrVC scheme. However, practical applications desire the algorithm to terminate within bounded steps. To meet the requirement, a finite number is used to specify the number of transparencies in the algorithm. The algorithm requires (x, y) obtained by solving L(t) or by looking up Table I. The outputs of Algorithm l are n' transparencies T1 , T2 ….. Tn and an index table Z , where Z[ω,h] is the index of the used

memory less sequence s[ω,h]to encode the secret pixel. In the first round, we use Algorithm 1 to generate n' transparencies and Z. If we need not to generate more transparencies in the future, is not required and removed. Otherwise, has to be stored in a safe section, and we can produce more transparencies T1 , T2 … Tn by utilizing Z

Algorithm 1. The algorithm of (t, ∞) OptPrVC scheme

Input: A binary secret image S, two positive integers t, n', and two vectors (X, Y).
Output: n' transparencies $T_1, T_2, \ldots, T_{n'}$; an index table Z.

```
1  for each pixel s[w,h] in S do
2    if s[w,h] = white then
3      Generate an integer z ∈ {t − 2k|k = 0,1,...,⌊t/2⌋}
       and P(z = t − 2k) = y_{t−2k}.
4    else
5      Generate an integer z ∈ {t − 1 − 2k|k =
       0,1,...,⌊(t − 1)/2⌋} and P(z = t − 1 − 2k) =
       −y_{t−1−2k}.
6    end if
7    Z[w,h] = z.
8    for k = 1 to n' do
9      Assign randomly T_k[w,h] to 0 or 1 where
       P(T_k[w,h] = 0) = x_z.
10   end for
11 end for
```

Fig. 1. Binary secret image.

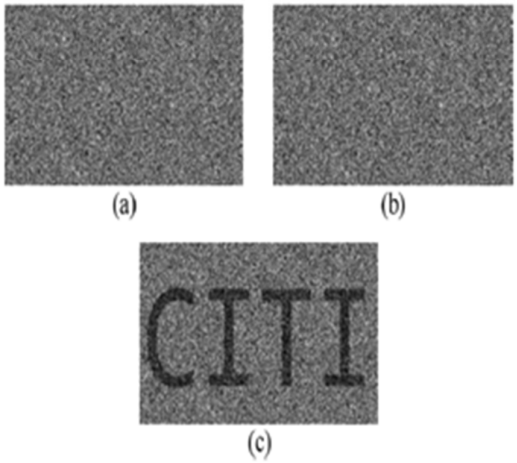


Fig 4 : Result of (2,∞) OptPrVC Scheme

(a)T1 (b)T2 (c) T1 Θ T2

ENCODING ALGORITHM OF (2,n) RG SCHEME PROPOSED BY CHEN AND TSAO [7]

Input: A binary secret image S, and a positive integers n.
Output: n transparencies $T_1, T_2, \ldots, T_n$.

1 Create T_1 by assigning each pixel to 0 or 1 and $P(T_1[w, h]=0)=1/2$.
2 **for** $k=2$ **to** n **do**
3 **for** each pixel $s[w, h]$ in S **do**
4 **if** $s[w, h]$ = white **then**
5 $T_k[w, h] = T_{k-1}[w, h]$.
6 **end if**
7 **if** $s[w, h]$ = black **then**
8 Assign randomly $T_k[w, h]$ to 0 or 1 where $P(T_k[w, h]=0)=1/2$.
9 **end if**
10 **end for**
11 **end for**

IV. CONCLUSION

In this paper, we have explored extended visual cryptography without magnification. We have shown that using an intelligent pre-processing of halftone images based on the characteristics of the original secret image, we are able to generate good quality images in the shares and the revert image. Note that other applications can also benefit from the pre-processing method, such as multiple image visual cryptography, which hides various images in shares.[8] Thus we propose an Extended visual cryptography scheme without pixel magnification for halftone images.

REFERENCES

[1] A. Ross and A. A. Othman, "Visual Cryptography for Biometric Privacy", IEEE Transactionson InformationForensics and Security, vol. 6, no. 1, pp. 70-81, 2011.
[2] C.L. Chou,"A Watermarking Technique Based on Nonexpansible Visual Cryptography", Thesis, Department of Information Management, National University, Taiwan, 2002.
[3] R. W. Floyd and L. Steinberg, "An Adaptive Algorithm for Spatial Gray Scale", in Proceedings of the Society for Information Display, vol.17, no. 2, pp.75-77, 1976.
[4] 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.
[5] N. Askari, C. Moloney and H.M. Heys,"A Novel Visual Secret Sharing SchemeWithout Image Size Expansion", IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), Montreal, pp. 1-4, 2012.
[6] T. H. Chen and K. H. Tsao, "Visual secret sharing by random grids revisited," *Pattern Recognit.*, vol. 42, no. 9, pp. 2203–2217, Sep. 2009.
[7] 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
[8] M. Naor and A. Shamir, "Visual cryptography", in EUROCRYPT '94 Proceedings, Lecture Notes in Computer Science, Springer-Verlag, vol. 950, pp. 1-12, 1995

BIOGRAPHIES

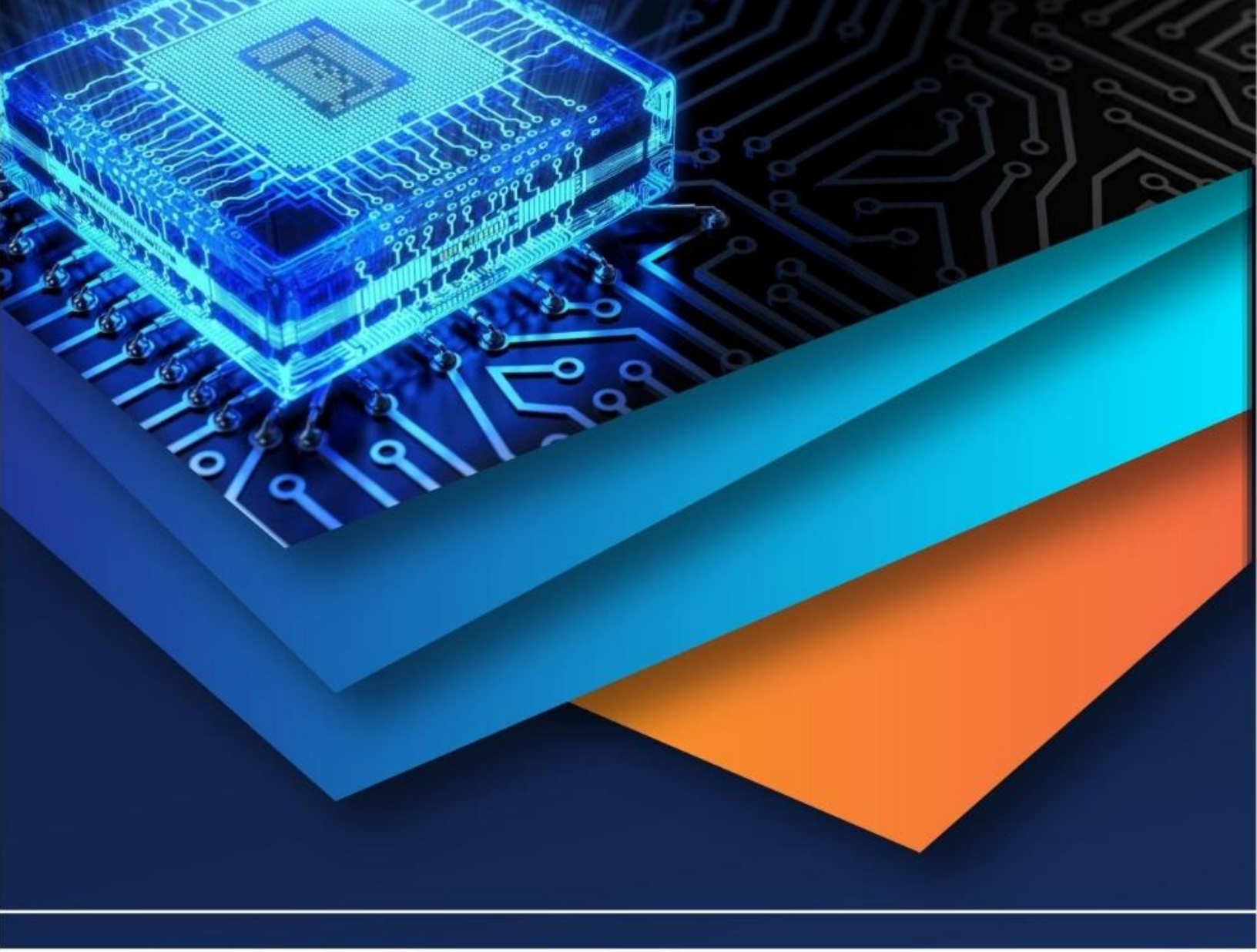
Umesh Anilkumar Jain pursuing the Bachelor of Engineering in Computer Engineering at Gokhale Education Society's R.H.Sapat College of Engineering,Management Studies and Research Certre , Nashik-42005, Maharashtra, India.

Vijendra Suresh Somwanshi pursuing the Bachelor of Engineering in Computer Engineering at Gokhale Education Society's R.H.Sapat College of Engineering, Management Studies and Research Certre , Nashik-42005, Maharashtra, India.

Rutuja Yogesh Ghule pursuing the Bachelor of Engineering in Computer Engineering at Gokhale Education Society's R.H.Sapat College of Engineering, Management Studies and Research Certre , Nashik-42005, Maharashtra, India.

Akshay Ravikumar Butte pursuing the Bachelor of Engineering in Computer Engineering at Gokhale Education Society's R.H.Sapat College of Engineering, Management Studies and Research Certre , Nashik-42005, Maharashtra, India.

Mr. S. R. Lahane is working as Assistant Professor in Computer Engineering at Gokhale Education Society's R. H. Sapat College of Engineering, Management Studies and Research Certre , Nashik-42005, Maharashtra, India.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY