International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST)
Vol. 1, Issue 1, April 2015

A novel visual cryptographic scheme using Floyd Steinberg halftoning and block replacement algorithms

Nisha Menon K[1], Minu Kuriakose[2]

Post-Graduate Scholar, ECE department, FISAT, Ernakulam, India[2]

Assistant Professor, ECE department, FISAT, Ernakulam, India[1]

***Abstract*— Visual Cryptography is a special encryption technique which is used to hide information in images in such a way that it can be decrypted by the human vision only if the correct key image is used. While visual cryptography was developed for application to binary images, and is inherently based on binary logical operations, it can be applied to grayscale images through their halftone representations. In this paper, a new method for processing halftone images is proposed that improves the quality of recovered secret images. The approach described in the paper mitigates the two traditional problems in visual cryptography of pixel expansion and loss of contrast.**

***Index Terms*—Cryptography, halftoning, image processing, secret sharing, visual cryptography(VC).**

I. INTRODUCTION

Increasing access to the Internet and information resources has a great impact on our everyday lives. As technology progresses and as more and more personal data is digitized, there is even more of an emphasis required on data security today than there has ever been. Various confidential data such as military maps and commercial identifications are transmitted over the Internet. While using secret images, security issues should be taken into consideration because hackers may utilize weak link over communication network to steal information that they want.

Cryptography is a well known approach to protect the data information by writing it in secret codes and transmitting in a secure way. The process of making the information unreadable is encryption or enciphering and the result of encryption is a ciphertext or cryptogram. Reversing this process and retrieving the original readable information is called decryption or deciphering. To encrypt or decrypt information, an algorithm or so called cipher is used. Cryptography protects the right to privacy and the right to communicate confidentially. Secure communications can protect one's intimate private life, business relations, and social or political activities.

Even with remarkable advances in computer technology, using a computer to decrypt secret image is infeasible in some situations. In these situations, the human visual system is one of the most convenient and reliable technique to do secret recovery. To deal with the security problems of secret images, various image secret sharing schemes have been developed. In the secret sharing scheme, original information to be encrypted is called as secret. After encryption, ciphers are generated and referred to as shares. Visual cryptography is a form of secret sharing. It is a cryptographic method that allows multiple entities to share the information required to reveal a secret image. Visual Cryptography is an emerging encryption technique to hide information in form of images in such a way that it can be decrypted by the human visual system**.** Using visual cryptography, the secret image is split into two or more separate random images called shares. To decrypt the encrypted information, the shares are stacked one on top of the other, and the hidden secret image appears. Due to its simplicity, anyone can physically manipulate the elements of the system, and visually see the decryption process in action without any knowledge of cryptography and without performing any cryptographic computations

Two main drawbacks of traditional visual cryptography are pixel expansion and low resolution. In this paper, a novel method is introduced which cancels the pixel expansion and improves the resolution of the image.

II. RELATED WORKS

The paper [2] explains the (k,n) secret sharing scheme. Within a secret sharing scheme, the secret is divided into a number of shares and distributed among *n* persons. When any *k* or more of these persons (where $k \leq n$) bring their shares together, the secret can be recovered. However, if k - 1 persons attempt to reconstruct the secret, they will fail. Due to this threshold scheme, such a secret sharing system is referred to as a (k, n)-threshold scheme or k-out-of-n secret sharing.

In the paper [2],Shamir formulated the definition of (k, n)-threshold scheme. The definition can be explained as follows: Let D be the secret to be shared among n parties. A (k,n)-threshold scheme is a way to divide D into n pieces D1, . . . ,Dn that satisfies the following conditions:

1. Knowledge of any k or more Di pieces makes D easily computable,

2. Knowledge of any k -1 or fewer Di pieces leaves D completely undetermined (in the sense that all its possible values are equally likely).

Visual cryptography (VC), first proposed in 1994 by Naor and Shamir [3], is a secret sharing scheme, based on black

International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST)
Vol. 1, Issue 1, April 2015

and-white or binary images. Secret images are divided into share images which, on their own, reveal no information of the original secret. Shares may be distributed to various parties so that only by collaborating with an appropriate number of other parties, can the resulting combined shares reveal the secret image. Recovery of the secret can be done by superimposing the share images and, hence, the decoding process requires no special hardware or software and can be simply done by the human eye.

All previous visual cryptography schemes were only limited to binary images. These techniques were capable of doing operations on only black and white pixels. It is not sufficient for real life applications. Chang-Chou Lin, Wen Hsiang Tsai in the paper [4] proposed visual cryptography for gray level images. In this scheme a dithering technique is used to convert gray level image into approximate binary image. Then existing visual cryptography schemes for binary images are applied to create the shares.

In the paper [5], a (k,n) threshold visual cryptographic scheme is described. In (2; 2) visual cryptography, both the shares are required to reveal secret information. If one share gets lost due to some technical problem, secret information cannot be revealed. So there is a restriction of keeping all the shares secure to reveal information and user can not afford to lose a single share. To give some flexibility to user, basic model of visual cryptography proposed by Naor and Shamir can be generalized into a visual variant of k out of n visual cryptography scheme. In (k, n) visual cryptography scheme, n shares can be generated from original image and distributed. Original image is recognizable only if k or more shares stacked together, where value of k is between 2 to n. If fewer than k shares stacked together, original image cannot be recognized. It gives flexibility to user. If user loses some of the shares still secret information can be revealed, if minimum k number of shares is obtained.

In (k, n) visual cryptography scheme, all n shares have equal importance. Any k out of n shares can reveal the secret information. It may compromise the security of system. To overcome this problem, G. Ateniese, C. Blundo, A. DeSantis, and D. R. Stinson extended (k, n) visual cryptography model to general access structure in the paper [6]. In general access structure scheme, given set of n shares is divided into two subsets namely qualified and forbidden subset of shares as per the importance of shares. Any k shares from qualified subset of shares can reveal secret information, but less than k shares from qualified subset of shares can not reveal any secret information. Even k or more shares from forbidden set can't reveal secret information.

Visual cryptography is of particular interest for security applications based on biometrics. The applications of visual cryptography in biometrics are explained in the paper [7]. The biometric information in the form of facial, fingerprint and signature images can be kept secret by partitioning into shares, which can be distributed for safety to a number of parties. The secret image can then recovered when all parties release their share images which are then recombined.

Although visual cryptography operates on binary images, it can be applied to grayscale images by using a halftoning algorithm to first convert the grayscale image to a binary image [8]. This allows for use of visual cryptography schemes to biometric images which are naturally and meaningfully grayscale, such as facial images. Hence, using halftoning techniques to convert grayscale images to binary images is a useful pre-processing step for visual cryptography.

In the paper [9], Floyd-Steinberg halftoning algorithm based on error diffusion is explained. The algorithm pushes (adds) the residual quantization error of a pixel onto its neighboring pixels. A Floyd Steinberg error diffusion matrix is used to distribute the error.

T.H. Chen, K.H.Tsao [10] have proposed n out of n and 2 out of n secret image sharing schemes which is based on the Random Grids .The main advantage in the technique is that there is no pixel expansion during encryption or decryption. Also codebook is used for encryption process. Where as in decryption process, the receiver has to superimpose one is by all or other one is at least two cipher-grids without any computation, resulted in getting good recognizable of secret image by the human visual system. The same authors have revisited the same paper called Visual secret sharing by random grids to enhance it to the extent of basic 2-out-of-2 scheme to the n-out-of-n scheme also 2-out-of-n scheme. To calculate the performance of this scheme resulted in a good value when using the random grids [11].

III. PROPOSED METHOD

The steps for implementing the proposed system are given in the fig. 1. The traditional cryptography cannot work with color images. So if an input image is a color image, it should be converted to binary form for applying visual cryptography. For this conversion the first step is grayscale conversion.

Compared to other halftoning algorithms, Floyd Steinberg algorithm is simple to implement and gives a moderate quality image. So for reducing the complexity of the proposed work, Floyd Steinberg is employed in the present work. Block replacement algorithms can be used for preprocessing. In this work three algorithms, SBR, BBR and Modified SBR are used. The block replacement algorithms compress the original image

In this work two out of two scheme with 4 subpixels is used. The share generation process can be divided into two white pixel processing and black pixel processing. In white pixel processing the number of white pixels is counted and the shares corresponding to it is assigned. The assignments of shares are in a random way. A similar process is applied in black pixel processing. The number of black pixels are counted and replaced with random shares corresponding to black. The inherent pixel expansion in generating shares is cancelled by the previous compression algorithm. As the compression algorithm compresses the image, the expansion effect is cancelled out. So the shares will have same dimensions as that of the original image.

International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST)
Vol. 1, Issue 1, April 2015

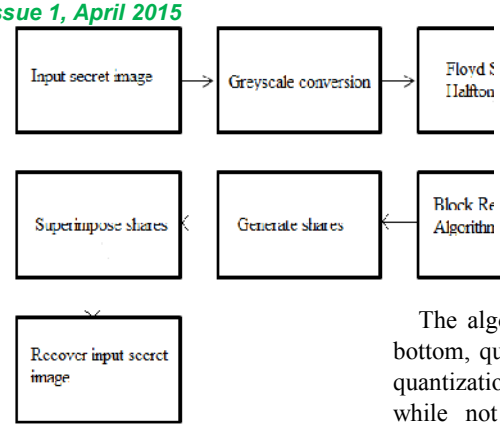


Fig. 1. Block diagram of proposed method

For recovering the secret input image, all the shares have to be stacked together. Here 2 shares are generated. So the shares are ORed. The resulting output is the recovered secret image.

A. Grayscale conversion

In photography and computing, a grayscale digital image is an image in which the value of each pixel is a single sample, that is, it carries only intensity information. Images of this sort, also known as black and white, are composed exclusively of shades of gray, varying from black at the weakest intensity to white at the strongest. Conversion of a color image to grayscale is not unique; a common strategy is to match the luminance of the grayscale image to the luminance of the color image. A gray color is one in which the red, green and blue components all have equal intensity in RGB space. The grayscale intensity is stored as an 8-bit integer giving 256 possible different shades of gray from black to white. Gray-level conversion is the process which converts the given original image to a 256 bits gray-level bitmap image.

B. Floyd Steinberg Halftoning

Floyd Steinberg halftoning is an error diffusion algorithm first published in 1976 by Robert W. Floyd and Louis Steinberg. The algorithm pushes the residual quantization error of a pixel onto its neighboring pixels. It spreads the debt out according to the distribution .If using the Floyd Steinberg matrix, the error occurred at the position (i, j) is weighted by 7/16 and added to the neighborhood pixel at (i+1, j). At the same time the error is also weighted by 1/16 and added to the neighborhood at (i+1, j+1) and so on. After the error has been diffused, the new input image I' is obtained. The same process moves to the pixel at the next position and performs the above described steps until all pixels have been processed

The fig.2 represents the error diffusion matrix in Floyd Steinberg algorithm. The pixel indicated with a star (*) indicates the pixel currently being scanned, and the blank pixels are the previously-scanned pixels.

$$\begin{bmatrix} \cdots & & * & \frac{7}{16} & \cdots \\ \cdots & \frac{3}{16} & \frac{5}{16} & \frac{1}{16} & \cdots \end{bmatrix}$$

Fig. 2. Floyd Steinberg error diffusion matrix

The algorithm scans the image from left to right, top to bottom, quantizing pixel values one by one. Each time the quantization error is transferred to the neighboring pixels, while not affecting the pixels that already have been quantized. Hence, if a number of pixels have been rounded downwards, it becomes more likely that the next pixel is rounded upwards, such that on average, the quantization error is close to zero.

The diffusion coefficients have the property that if the original pixel values are exactly halfway in between the nearest available colors, the dithered result is a checkerboard pattern.

C. Block Replacement Algorithms

After creating a halftone image, in order to preserve the image size when applying visual cryptography, simple methods can be applied. For example, a basic, secure method that is easy to implement is based on a block-wise approach to pre-processing the binary halftone image prior to applying visual cryptography. In this paper, block replacement algorithms such as Simple Block Replacement (SBR), Balanced Block Replacement (BBR) and Modified SBR are introduced.

1) Simple Block Replacement (SBR)

The SBR scheme considers groups of four pixels from the halftone secret image in one 2 × 2 block, referred as a secret block, and generates the shares block by block (rather than pixel by pixel). As each secret block with four pixels encodes into two secret shares each containing four pixels, the size of the reconstructed image is the same as the original secret image after stacking the two shares together. In this technique, all the secret blocks in an image need to be processed before visual cryptography encoding and each secret block is replaced by the corresponding predetermined candidate, which is a block with 4 white pixels (a white block) or a block with 4 black pixels (a black block).

The block replacement process in the SBR pre-processing scheme is based on a number of black and white pixels in each secret block. The SBR scheme is illustrated in fig. 3. If the number of black pixels in a secret block is larger than or equal to 2, the secret block converts to a black block. If the number of black pixels in a secret block is less than or equal to 1, it is converted to a white block. This step produces a new secret image which contains only white and black blocks.

International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST)
Vol. 1, Issue 1, April 2015

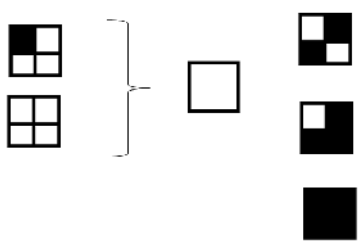


Fig. 3. Implementation of SBR

The image obtained from this step is referred to as a processed secret image. The SBR approach is straightforward and is very effective for unprocessed binary secret images which have large numbers of all white and all black blocks. However, for halftone images, with high variability in the distribution of black and white pixels within each secret block, the resulting processed secret image is generally poor, being darker than the original image, with poor contrast, causing the loss of many fine details in the images.

2) Balanced Block Replacement (BBR)

A novel and effective method for replacing the candidate blocks of a halftone secret image, is referred to as the balanced block replacement (BBR) method. The novel aspect in this approach is to perform the block replacement such that there is a better balance of white and black in the processed secret image. The previously described SBR scheme results in darker images, since blocks which contain two white and two black pixels are converted to a black block. The blocks of two white and two black pixels are referred to as candidate blocks. In the BBR approach, white and black are balanced in the processed image by assigning some candidate blocks to black and others to white. Although doing the candidate block assignment randomly to black or white improves the visual quality of the processed secret image, even better visual results can be achieved using an intelligent block replacement approach that considers the characteristics of the original image in determining whether a candidate block should be assigned to black or white. The block replacement approach proposed here tries to keep 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 secret image. Therefore, the resulting recovered image is closer in quality to the original grayscale image.

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 cluster. In the second step, the number of black pixels in each cluster from the halftone image are counted and saved in a template. This number is the threshold value for that cluster. The next step is to classify all the secret blocks containing 1 black pixel. If the secret block contains 1 black pixel, it is converted to a white block. The image obtained from this step is referred to as the initial processed image. In fig. 4, the initial processing is illustrated.

The third step starts from the first block in the top left of the first cluster of the initial processed image. The processing of the blocks in each cluster starts from the top left block, and then moves from left to right and top to bottom in raster format. When the first candidate block in a cluster is identified, the number of black pixels in the cluster is counted. The number of black and white pixels in each cluster of the initial processed image should be kept as close as possible to the corresponding threshold value from the cluster of the original halftone image. Therefore the number of black pixels in the case of changing the candidate block to a black or white block is computed and is compared to the threshold value that was derived for the same cluster in the original halftone image. If the corresponding candidate block converts to a black block, 2 black pixels will be deducted from a cluster. The conversion is based on the smallest difference between the threshold and the number of black pixels in the image being processed. If changing the candidate blocks to black makes this difference smaller, the candidate block is converted to a black block. Similarly, if turning the candidate block to white makes this difference smaller, the block converts to a white block. In the case that turning the candidate to black or white produces the same difference, the block randomly converts to either a black or white block.

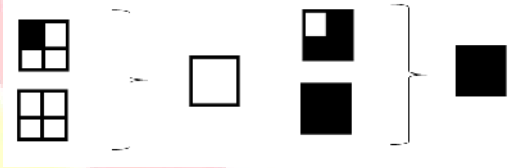


Fig. 4. Illustration of initial processing in BBR

3) Modified Simple Block Replacement

This is a modification of Simple Block Replacement method. When the number of black pixel is greater than two or less than two, this algorithm will follow same the initial processing steps. The difference is when the number of black pixel is equal to two. When this condition is encountered, a random number is generated. If the random number is closer to 1, then the block is assigned as a white block. If the random number is closer to zero, then it is assigned as a black block. The performance of the new scheme is superior to SBR but inferior to BBR. But in the terms of complexity, the modified SBR is found to be less complex because there is no more cluster formation.

D. Recovery of input image

The generated shares are superimposed at the receiver to get the secret image. The shares are overlaid in the correct alignment to produce the original secret. The mathematical function used for overlapping is the OR function. The output image will have the same size as that of the shares.

IV. Experimental Results

The input given is a color image 'pepper.png' It is shown in fig. 5(a). The input image is then converted to grayscale image using the inherent function available in matlab. The grayscale image is shown in

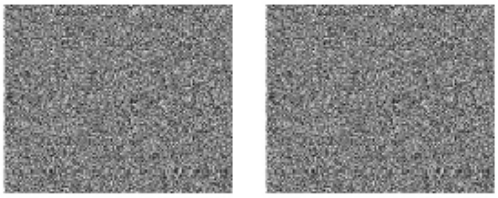
International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST)
Vol. 1, Issue 1, April 2015

(a) (b)

Fig. 5. (a) input image, (b) grayscale image

The 2 shares generated are shown in fig. 6. It can be observed that the shares are random and don't reveal any information about the input secret image.

. The amount of black pixel is high in SBR processed output. Modified SBR gives a better output compared to SBR. The fig.7 shows the results of SBR, modified SBR, BBR. The BBR algorithm gives the best result compared to other block replacement algorithms.



(a) (b)

Fig. 6. shares (a) share 1, (b) share 2

(a) (b) (c)

Fig. 7. Result of different block replacement algorithms (a) Result of SBR, (b) Result of modified SBR, (c) Result of BBR

A significant improvement can be observed in the visual quality of the reconstructed image in comparison to the SBR method. Compared to Balanced Block Replacement algorithm, modified SBR is less complex. But in performance modified SBR is inferior to BBR.

V. Conclusion

In this paper, visual cryptography without pixel expansion is proposed. An effective halftoning by Floyd Steinberg error diffusion is used here. It can improve the contrast of the image. By pre-processing of halftone images, using block replacement algorithms, the pixel expansion is cancelled.

Acknowledgment

This work is supported and guided by my research guide. I am very thankful to my guide Ms. Minu Kuriakose, Assistant Professor, Electronics and Communication Department, Federal Institute of Science and Technology,(FISAT) Mookkannoor for her guide and support.

References

[1] N. Askari, C. Moloney and H.M. Heys,"An extended visual cryptographic scheme without pixel expansion for halftone images" *IEEE Canadian Conference on Electrical and Computer Engineering (CCECE),* Montreal, pp. 1-4, 2013.

[2] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, pp.612–613, 1979.

[3] M. Naor and A. Shamir, "Visual cryptography", *in EUROCRYPT '94 Proceedings*, Lecture Notes in Computer Science, Springer-Verlag, vol. 950, pp. 1-12, 1995.

[4] Chang-Chou Lin, W.-H. T. (July 2002). "Visual Cryptography for gray-level image"

[5] S. Cimato, R. De Prisco, and A. De Santis, "Optimal colored threshold visual cryptography schemes," *Designs, Codes, Cryptogr.*, vol. 35, pp. 311–335, 2005.

[6] Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual cryptography for general access structures," *Inf. Comput.*, vol. 129, pp. 86–106, 1996.

[7] 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.

[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] 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.

[10] T.H. Chen, K.H. Tsao, "Visual secret sharing by random grids ", *Pattern Recognition*, vol. 42, no.9, pp.2203–2217, 2009.

[11] T.H. Chen, K.H. Tsao, "Visual secret sharing by random grids revisited", *Pattern Recognition*, vol. 42, no.9, pp.2203–2217, 2009

Nisha Menon K received the B.Tech degree in Electronics and Communication Engineering from Calicut University, Kerala, India, in 2013. Currently, she is post graduate student with the Department of Communication Engineering, Federal Institute of Science and Technology (FISAT), Kerala, India. Her current research area includes encryption-then-compression algorithms.

Minu Kuriakose received the Bachelor's degree in Electronics and Communication Engineering from M.G. University and M.Tech in Computational Engineering and Networking from Amrita University, Coimbatore in 2009. Since 2009, she has been working as Assistant Professor in Federal Institute of Science and Technology (FISAT), Kerala, India.