ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 352 - 356 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

A VISUAL CRYPTOGRAPHY SCHEME WITH LAYERED EXPANSION FOR SECRETHALFTONE IMAGES

M. KarthikBabu[1] , S. Amarnath Babu[2]
Pursuing M.Tech, SACET, Chirala, Andhra Pradesh, India[1]
Assoc. Professor, SACET, Chirala, Andhra Pradesh, India[2]

***Abstract* - Visual cryptography may be a cryptographical technique that permits the visible data like pictures, words etc.., to be hided in such the way that decipherment becomes a mechanical operation that doesn't need a laptop. Secret pictures area unit divided into share pictures that, on their own, reveal no data of the initial secret. Shares could also be distributed to numerous parties in order that solely by collaborating with Associate in nursing acceptable range of different parties, willthe ensuing combined shares reveal the key image. Recovery of the key is done by superimposing the share pictures and, hence, the decipherment method needs no special hardware orsoftware packageand might be merely done by the human eye. Visual cryptography is of specific interest for security applications supported life science**

***Key Words* — cryptography, image processing, visual cryptography, secret sharing.**

INTRODUCTION

Visualcryptography is a cryptographic technique which allows the visible information like images, words etc.., to be hided in such a way that decoding becomes a mechanical operation that does not require a computer.Secret images are divided intoshare images which, on their own, reveal no information ofthe original secret.Shares may be distributed to various partiesso that only by collaborating with an appropriate numberof other parties, can the resulting combined shares reveal thesecret image.Recovery of the secret can be done by superimposingthe share images and, hence, the decoding processrequires no special hardware or software and can be simplydone by the human eye.Visual cryptography is of particularinterest for security applications based on biometrics [3]. The secret image can then recovered when all partiesrelease their share images which are then recombined.

Visual Cryptography provides a friendly setting subsume the photographs. Typically cryptography tools support only 1 reasonable format. Our application supports .gif and .png formatted pictures.

VCS of Associate in Nursing EVCS,we tend to mean a standard VCS that have an equivalent access structure with the EVCS. Generally, Associate in Nursing EVCS takes a secret image and original share pictures as inputs, and outputs shares that satisfy the subsequent 3option:

1. Any qualified set of shares will recover the key image;
2. Any verboten set of shares cannot acquire any info of the key image apart from the key image apart from the scale of the image.
3. All the shares are important pictures.

An example of ancient (2, 2) VCS will be found in Fig., where, typically speaking, a VCS suggests that any out of sharesmight recover the key image. Within the theme of Fig., shares (b) and (c) are distributed to 2 participants on the Q.T., and every participant cannot get any info regarding the key image, however when stacking shares (b) and (c), the key imagewill be determined visually by the participants.

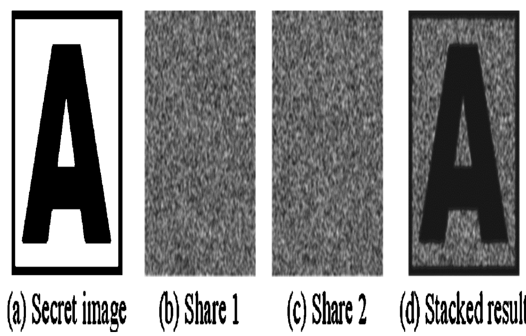


Fig: a) Secret Image b) Share 1 c) Share 2 d) Result after placing the share 1 and share2.

PRE-PROCESSING HALFTONE IMAGES

The applying of visual cryptography to grey scale pictures by 1st changing the photographs to a binary image employing a halftoning algorithmic program. The task of the project is to implement an algorithm, which should be fast and the printed images must look good based, on human visual perception.In this project, we survey some of the existing methods.Further, based on2-by-2 block replacement method, we propose an improved algorithm.Theimprovements can be divided into three major parts. They are:

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 352 - 356 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

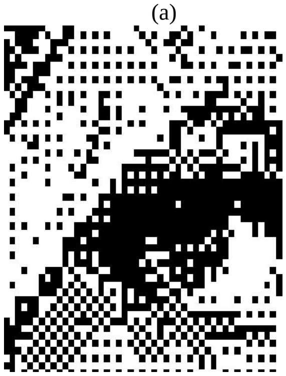
1. Adaptive gray level region definition
2. Inclusion of the nearest neighbours in the analysis before halftoning
3. Parallelize the algorithm in order to speed up the conversion.

WHAT IS HALFTONING AND HOW IT WORKS

The grayscale digital image consists of 256 gray levels, while the black and white printers only have one colored ink. So, there is a need to replace wide range of grayscale pixels for printers. These 256 levels of gray should some-how be represented by placing black marks on white paper. Halftoning[6] is a representation technique to transform the original continuous tone digital image into a binary image only of 1's and 0's consisting. The value 1 means to fire a dot in the current position and 0 means to keep the corresponding position empty.

Since the human eyes have the low pass spatial-frequency prosperity, human eyes perceive patches of black and white marks as some kind of average grey when viewed from sufficiently far away. Our eyes cannot distinguish the dots patterns if they are small enough. Instead, our eyes integrate the black dots and the non-printed areas as varying shades of gray. Fig 2(b) shows a typical halftoning image. Zooming in a part of the halftoning image, we can see that the image is actually structured by a certain strategy of distributed black dots.

(a) (b)



(c)

Fig 2: (a) The original image; (b) The halftoning image; (c) An enlargement of (b)

Here we are using the Block Replacement Method for pre-processing the halftone images.

AN IMPROVED PRE-PROCESSINGSCHEME

Block replacement halftoning is a commonly used halftoning technique. Inthis method each pixel in the original image is replaced by one of the defined set of binary blocks. The dimension of the patternsis determined by screen frequency and the print resolution [1]. For simplicity, assume that each pixel is going to be replaced by a 2X2 matrix. Sincethe dimension of the matrix is 2X2 then only five different gray levels canbe represented by the set of matrices, see Fig 3. The pixel belong to oneof the five gray level regions is replaced by the corresponding predeterminedcandidate. Fig 3 illustrates how this method works. In this illustrationonly the representation for the first and the last pixel are shown. The sameis done for the rest of the original image. In Fig 2 the left is the imagehalftoned by a 2-by-2 block replacement halftoning, and the right is by a3-by-3 block replacement. The 3-by-3 block replacement can represent tendifferent gray levels. Comparing the two images (a) and (b), we see that the3-by-3 block replacement can keep more details than 2-by-2 replacement,the bigger number of gray levels, the higher resolution. In contrast to theordered dithering method, the arrangement of the black micro dots in thepatterns does not have necessarily to be clustered or to be dispersed. Dueto the low-pass spatial frequency property of the human eye, the same graylevel can be represent by two different patterns, any of which can possiblybe arranged as a clustered dot and another as a dispersed dot. The choiceof the patterns has an impact on the characteristics of the final halftoningimage. This will be describes in detail in the next section.

(a) (b)

Fig 3: Halftoning images by block replacement. In (a), the candidatesare 2 x 2, hence five levels of gray. In (b), the candidates are 3 x 3, hence10 levels of gray.

Example for Block Replacement is shown in the following Fig.

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 352 - 356 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

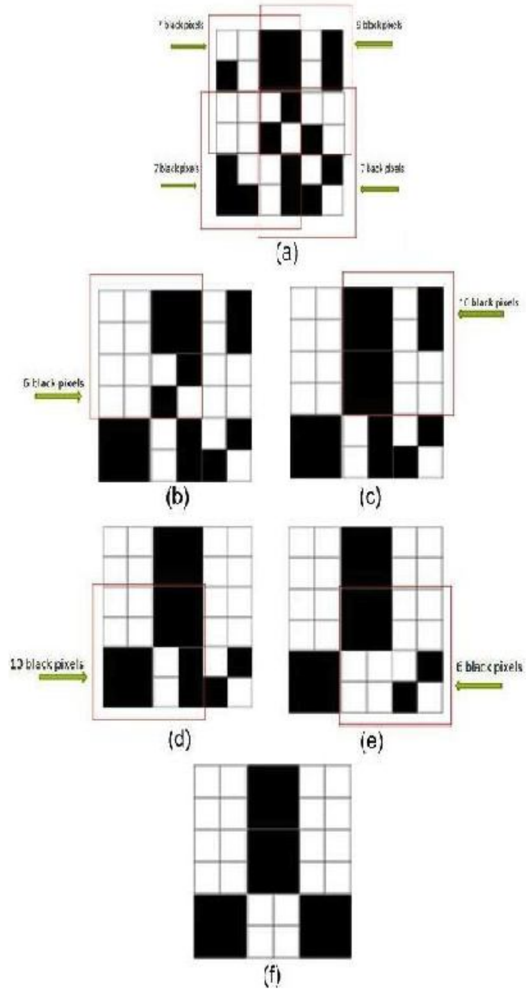


Fig: Example for Block Replacement

EXTENDED VISUAL CRYPTOGRAPH

Extended Visual Cryptography may be a sort of cryptography that encodes variety of pictures within the method thatonce the pictures on transparencies area unit stacked along, the hidden message seems while not a trace of originalpictures. The coding is completed directly by the human sensory system with no special cryptologic calculations. Generally, visual cryptography suffers from the deterioration of the image quality. This project additionally describesthe strategy to enhance the standard of the output pictures. The trade-off between the image quality and therefore thesecurity area unit mentioned and assessed by observant the particular results of this technique. What is more, theimprovement of the image quality is mentioned.

EVCS is versatile within the sense that there exist 2 trade-offs between the share constituent growth and therefore thevisual quality of the shares and between the key image constituent growth and therefore the visual quality of the shares. This flexibility permits the dealer to settle on the right parameters for various applications. Comparisons on the experimental results show that the visual quality of the share of the projected embedded EVCS is competitivethereupon of the many of the well-known EVCSs within the literature.

PROPOSED SYSTEM:

Visual cryptography may be a quite cryptography that may be decoded directly by the human sensory system with nonespecial calculation for coding. As shown in below Fig, our visual cryptographysystem takes 3 footage as an input and generates 2 pictures that correspond to 2 of the 3 input footage. The third image is reconstructed by printing the 2output pictures onto transparencies and stacking them along, this sort of visual cryptography, that reconstructs the image by stacking some substantive pictures along, is especially called Extended VisualCryptography [5]. In this project, the pictures shown on the outputimages are called *sheets* and the resulting image reconstructedby stacking the two sheets together is called the *target*.Previous works on the extended visual cryptography deal withbinary images such as text images, but natural images such asphotographs are difficult to handle in such scheme. Thisproject establishes the extended visual cryptography themefor natural pictures. Generally, visual cryptography suffersfrom the deterioration of the image quality. This project additionallydescribes the tactic to enhance the standard of the outputimage.

Proposedsystem **Visual cryptography** provides friendly surroundings to trout out pictures. Our application has been developed exploitation swing and applications programme technologies, thus provides a friendly surroundings to users.

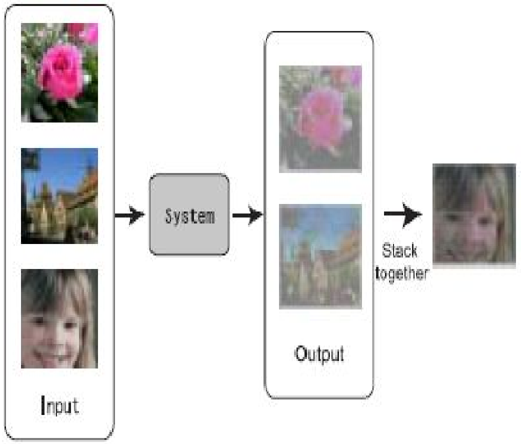
VISUAL SECRET SHARING SCHEME:

The basic model of the visual cryptography consistsof a several number of visible sheets. On everyvisibility a cipher text is written that is differentfrom random noise. The hidden message is reconstructed bystacking a particular variety of the transparencies and viewingthem. The system can be used by anyone without anyknowledge of cryptography and without performing anycryptographic computations. Naor and Shamir have developedthe Visual Secret Sharing Scheme (VSSS) to implement thismodel. In k out of n VSSS (which is also called (k, n) scheme),a binary image (picture or text) is transformed into n sheets oftransparencies of random images. The original image becomesvisible when any k sheets of the n transparencies are puttogether, but any combination of less than k sheets cannotreveal the original binary image.In the scheme, one pixel of the original image isreproduced by m sub pixels on the sheets. The pixel isconsidered “on” (transparent) if the number of transparent subpixels is more than a constant threshold, and “off” if thetransparent sub pixels is less than a constant lower threshold,when the sheets are stacked together. The contrast α is thedifference between the on and off threshold number oftransparent pixels. Ateniese et

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 352 - 356 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

al. has extended the (*k*, *n*) VSSSto general access structures where everwill specify allqualified and out subsets of *n*participants. Drostethought about the matterof sharing more than one secret imageamong a set of participants and proposed a method toreconstruct different images with different Combination ofsheets.



The Basic Idea of the Proposed System

EXTENDED VISUAL CRYPOTOGRAPHY:

Naor associating in nursing and Shamir [2] have mentioned an extension of themodel which conceals the terribly existence of the key image. That is, each sheet carries some meaningful imagesrather than random dots. They referred to the (2, 2) examplewith the number of sub pixels m = 4. Ateniese has formalizedthis framework as *the Extended Visual Cryptography* [8]anddeveloped a Scheme for general access structures.They also discuss the trade-off between the contrastof the each images on the sheets and that of the resultingimage when stacked together in(*k*, *k*) cases.

APPLICATION TO EXTENDED VC

GRAY SCALE CONVERSION:

In photography and computing, a grayscale digitalimage is a picture which the worth of every pixel may be asingle sample, that is, it carries solelyabout the picture information. Images of this sort, also known as black-and-white [8], are composed having the shades of gray,varying from black at the weakest intensity to white atthe strongest.

The grayscale images are different from black and white images, which in the context of computer imaging are images with only the two colors, black and white images, which in the context of computer imaging are images with only the two colors, black and white. Grayscale images have many shades of gray in between. Grayscale images are also called monochromatic, denoting the presence of only one (mono)color (chrome).

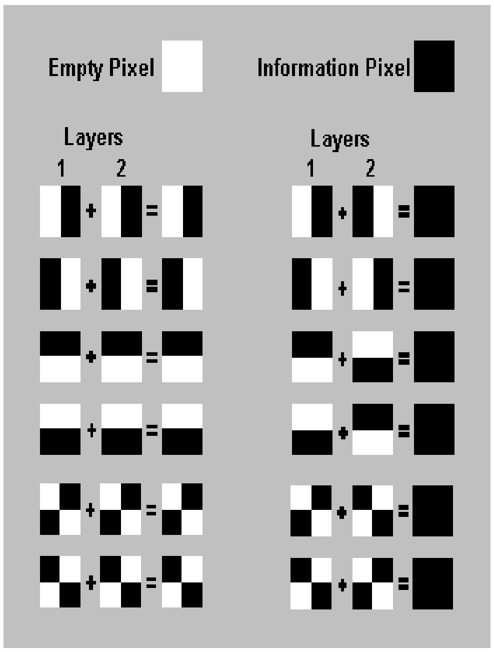
Conversion of a color image to grayscale is notunique; a common strategy is to match the luminance ofthe grayscale image to the luminance of the colorimage. In fact a gray color is one in which the red,green and blue components all have equal intensity inRGB space. The grayscale intensity is stored as an 8-bitinteger giving 256 possible different shades of grayfrom black to white. Gray-level conversion is theprocess which converts the given original image to a256 bits gray-level bitmap image.

Steps of grayscale algorithm:

Step 1: Give the height and width of the image.
Step 2: X and Y axis are declared.
Step 3: The starting position of the X and Y axisare '0'.
Step 4: Now the starting position is incremented to '1'.
Step 5: Now we are getting the position of x and y values of X and Y axis.
Step 6: Check the color of the getting position whether it is black or white.
Step 7: If the color of the position is near to black change it as to pure black.
Step 8: Else if the color of the position is near to white change it as to pure White.
Step 9: Procedure will continued until the process completed.

IMAGE ENCRYPTION:

In cryptography, encryption is the process of the conversion of information from a reading state to non reading state. In an encryption scheme, the message orinformation is encrypted using an encryption algorithm,turning it to an unreadable cipher-text. The aim this technique is to cover the information and the code will be send to the exact user. The user only sees the hidden image.



Steps of encryption algorithm:

Step 1: Get width and height of the image

ISSN 2278-3091

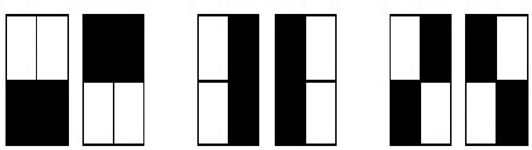
International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 352 - 356 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

Step2: Horizontal block=image width/2
Step3: Vertical block =image height/2
Step 4: Number of block = horizontal block Xvertical block
Step 5: For n=0 to no.of.block-1
For x=0 to n-1
For y=0 to n-1
Encrypt pixel using position (x, y)

IMAGE DECRYPTION:

The decryption of the image will be done byoverlapping the shares, without removing cover images,by means of that we can avoid pixel expansionproblems. Where removing cover images results inchange in the display quality of the recovered image.When we place both the shares one over another withproper alignment, we can interpret the original image.
FOR BLACK AND WHITE IMAGES:

In the original encryption, the problem can be considered as a (2, 2) secret sharing. The solution of the (2, 2) black-and-white VCS scheme by either dividing one pixel into two subpixels or four subpixels in the two shares. So the size of thesuperimposed image is expanded [4] by a factor of 4. The following Fig. shows all the possible arrays of the four subpixels.



The Six Arrays of Four Subpixels

Randomly choose an array from Fig. for a pixel in the secret image, as the first share. The second share is identical with the first one if the original pixel is white and if the original pixel is black, the second share is complementary with the first one. When we superimpose the two shares, the white color is recovered as medium gray and the black color is recovered as completely black. Secret sharing improves the reliability and robustness of secure key management.

Example: Consider the following situation: If the only key that provides access to some important data is lost somewhere, then that important data will become inaccessible. Thus this problem can be resolved by dividing the key into pieces and then distributing them to different persons so that any pre-specified set of persons can recover the key jointly.

CONCLUSION

In this paper, we've explored extended visual cryptography while not enlargement. We've shown that using an intelligent pre – processing of halftone pictures supported the characteristics of the first secret image, we tend to square measureable to manufacture smart quality images within the shares and therefore the recovered image. Note that alternative applications may also enjoy the pre-processing approach, like multiple image visual cryptography, that hides multiple pictures in shares.

REFERENCES

[1] S. Gooran, Digital Halftoning, Thesis, Linkoping University, Linkoping, Sweden.

[2] M. Naor and A. Shamir, "Visual cryptography," in *Proc. EUROCRYPT' 94*, Berlin, Germany, 1995, vol. 950, pp. 1–12, Springer-Verlag, LNCS.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] M. Nakajima and Y. Yamaguchi, Extended Visual Cryptography for Natural Images, in Proceeedings of WSCG, pp. 303-310, 2002.

[9] C.L. Chou,"A Watermarking Technique Based on Nonexpansible Visual Cryptography", Thesis, Department of Information Management, National University, Taiwan, 2002.

[10] 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.

AUTHORS:

Amarnath Babu S is presently working as associate professor, Dept of Computer Science and Engineering, in St.Ann's College of Engineering and Technology, Chirala. He Guided Many UG and PG Students. He has More than 11 Years of Excellence in Teaching. He published 6 International Journals.

Karthik Babu Manam received the B.Tech degree in Electronics &Instumentation Engineering from AcharyaNagarjuna University, in 2011 & pursuing his M.Tech in Computer Science & Engineering from JNTU Kakinada.