International Journal of Computers & Technology
Volume 5, No. 2, May -June, 2013, ISSN 2277-3061

EXTENDING THE VISUAL CRYPTOGRAPHY ALGORITHM USING IMAGE WATERMARKING TECHNIQUE

Dr.V.R.Anitha, M.Tech, Ph.d [1], Dilip kumar Kotthapalli [2]

[1] Professor of ECE, Department of Electronics and Communication Engineering, Sree Vidyanikethan Engineering College, TIRUPATI – 517 102, A. P., INDIA

[2] M.Tech student, Department of Electronics and Communication Engineering, Sree Vidyanikethan Engineering College, TIRUPATI – 517 102, A. P., INDIA

E-mail: [1] anithavr@gmail.com , [2] shekardlip@gmail.com

Abstract - Visual cryptography is a secret information sharing technique which shares the information in the form of images. It generates noise-like random pixels on share images to hide secret information which on overlay decrypt the information. This technique is known as conventional visual secret sharing schemes. It suffers a management problem, because of which dealers cannot visually identify each share. This problem is solved by the extended visual cryptography scheme (EVCS), which adds a meaningful cover image in each share. While removing the extra cover image it produces extra noise or degrades the hidden image quality. So we propose a new image watermarking technique in this Visual Cryptography Algorithm that places a small image on the noisy image pair at the bottom right corner. So that the cover images need not be removed and it doesn't degrade resolution of the secret image.

Index Terms **-** pixel expansion, watermarking, visual cryptography

I. INTRODUCTION

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer. One of the best-known techniques has been credited to Moni Naor and Adi Shamir, who developed it in 1994. They demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n-1 shares reveals no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear. Using similar idea, transparencies can be used to implement a one-time pad

encryption, where one transparency is a shared random pad, and another transparency acts as the cipher text.

F. Liu, C. Wu, and X. Lin, “Step construction of visual cryptography schemes,” in Mar. 2010 proposed a recursive approach to construct VCS for GASs. By using the GAS, dealers can define reasonable combinations of shares as decryption conditions rather than specifying the number of shares.

Conventional VSS schemes generate noise-like random pixels on shares to hide secret images. In this manner, the secret can be perfectly concealed on the share images. However, these schemes suffer from a management problem dealers cannot identify each share visually. Hence, researchers have developed the extended visual cryptography scheme as proposed in “Extended capabilities for visual cryptography,” 2001 by G. Ateniese, C. Blundo, A. D.Santis, and D. R. Stinson, which adds a meaningful cover image on each share to address the management problem.

Visual Cryptography (VC) aims to share a secret message between several shadow images (SI, sometimes named transparencies) in accordance with the initial scheme. That algorithm is known to be very effective because no information about the message transmitted what-so-ever leaks into any of the SI’s. This differs from the technique known as watermarking.

In VC, all required SI’s need to be present, and need to be overlaid for the message to appear. In a VC scheme, each SI is a random distribution of black-and-white subpixels. All subpixels are independent from each other and therefore one SI alone leaks strictly no information. To reveal the message a minimal number of SI’s must be stacked together and duly registered

The pixel expansion problem is a common disadvantage with most of the VSS schemes. When the VC -based approach is employed, each secret pixel within a secret image is encrypted in a block consisting of sub pixels in each constituent share image. Thus, the area of a share is times that of the original secret image. The contrast of the recovered images will be decreased simultaneously.

The pixel expansion problem not only affects the practicability of storage/transmission requirements for shares but also decreases the contrast of the recovered secret images. To the best of our knowledge, the existing EVCS algorithms for GASs cannot avoid the pixel expansion problem.

II.EXISTING SYSTEM

Conventional VSS schemes generate noise-like random pixels on shares to hide secret images. In this manner, the secret can be perfectly concealed on the share images. However, these schemes suffer from a management problem dealers cannot identify each share visually. Hence, researchers have developed the extended visual cryptography scheme, which adds a cover image to share images but adding the cover images changes the aspect ratio of the image. There are mainly two limitations- image shares have management issues and additional information causes pixel expansion problem.

III.PROPOSED SYSTEM

The first phase of the algorithm, which uses optimization techniques for a given access structure, constructs a set of noise-like shares that are pixel expansion free. We identified and formulated the problem in this phase as a combinatorial optimization problem and then developed a simulated-annealing based algorithm to solve it. The second phase of the algorithm directly adds a cover image as a watermark on each share. In this manner, the

International Journal of Computers & Technology
Volume 5, No. 2, May -June, 2013, ISSN 2277-3061

pixel expansion can be removed entirely. Here pixel expansion is solved and display quality of cover image is adjustable.

IV. SYSTEM ARCHITECTURE

In summary, phase I of the proposed algorithm contains two subprocedures: first, finding the number of basis shares n and a corresponding construction set C for a VCS. We develop a GAS solver as shown in fig.1, to deal with these works. Second, basis shares that were yielded by the constructions of VCS and the construction set C will be utilized to obtain uncovered I-shares. This work will be carried out by the encryptor and the share synthesizer, as shown in fig. 1. Here the construction set C holds the relation between the basis shares and the I-shares.

Liu's approach had some additional drawbacks: first. The participants may take multiple share images with different pixel expansions for one secret image. This differs from conventional VC schemes and will increase administrative inconvenience and difficulty. Second. The decryption process is more complicated than conventional VCSs and needs the help of other vice.

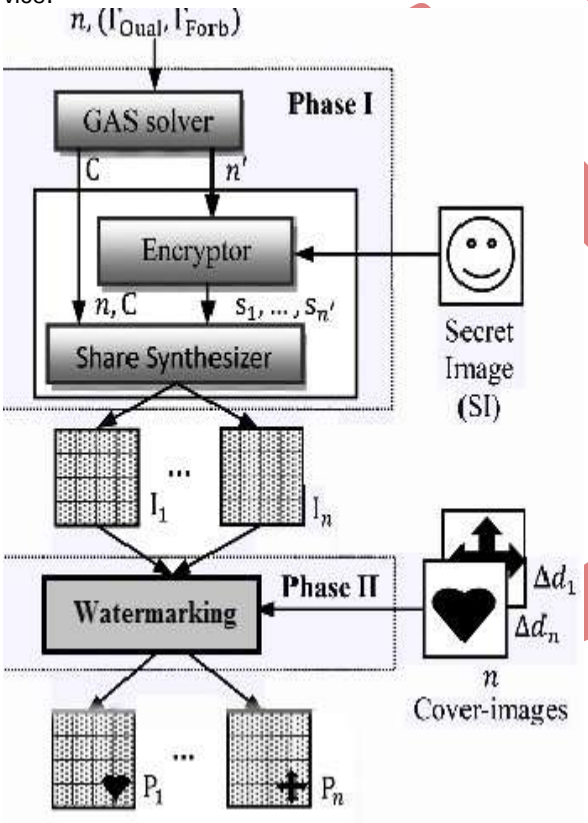


Figure 1 System Architecture

V. DESIGN OF MODULES

The proposed work is divided into four modules as 1. Gray Scale Conversion, 2. Image Encryption, 3.Water Marking Technique, 4. Image Decryption.

1. 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.

In this module color image is converted to grayscale. Grayscale images are distinct from one-bit bi-tonal black-and-white images, which in the context of computer imaging are images with only the two colors, black and white (also called bi-level or binary images).

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. In fact a gray color is one in which the red, green and blue components all have equal intensity in RGB space.

Algorithm 1: Grayscale Conversion

Step 1: Get dimension of the uploaded image
Step 2: Declare to variable X and Y representing x axis and y axis.
Step 3: Set initial position of X and Y to '0'
Step 4: Increment the value of x and y by '1'
Step 5: Get the pixel value of x and y
Step 6: Check to which the pixel value is near-by to white or black
Step 7: Change the value to black if it is near to black
Step 8: Else change the value to the white if it is near to white
Step 9: Repeat till all the pixels are converted.

2. Image Encryption

In an encryption scheme, the message or information is encrypted using an encryption algorithm, turning it to an unreadable cipher-text. This image is divided into n slides called transparency. Each pixel of the message appears in each transparency in a different modified version. For getting the original information from transparencies, all of them are stacked together with proper alignment.Each pixel of the images is divided into smaller blocks. There are always the same number white (transparent) and black blocks. If a pixel is divided into two parts, there are one white and one black block. If the pixel is divided into four equal parts, there are two white and two black blocks.

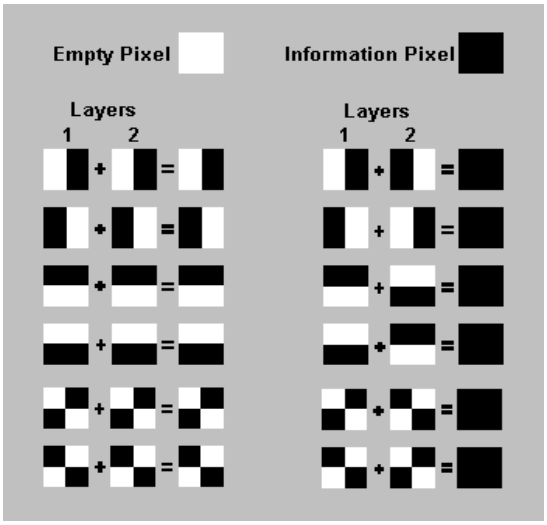


Figure 2 shares synchronization

In the table on the right we can see that a pixel, divided into four parts, can have six different states. If a pixel on layer 1 has a given state, the pixel on layer 2 may have one of two states: identical or inverted to the

International Journal of Computers & Technology
Volume 5, No. 2, May -June, 2013, ISSN 2277-3061

pixel of layer 1. If the pixel of layer 2 is identical to layer 1, the overlayed pixel will be half black and half white. Such overlayed pixel is called grey or empty. If the pixels of layer 1 and 2 are inverted or opposite, the overlayed version will be completely black. This is an information pixel.

We can create the two layers. One transparent image, layer 1, has pixels which all have a random state, one of the six possible states. Layer 2 is identical to layer 1, except for the pixels that should be black (contain information) when overlayed. These pixels have a state that is opposite to the same pixel in layer 1. If both images are overlayed, the areas with identical states will look gray, and the areas with opposite states will be black.

Black + Black = Black
White + Black = black
Black + White = black
White + White = White

If Visual Cryptography is used for secure communications, the sender will distribute one or more random layers 1 in advance to the receiver. If the sender has a message, he creates a layer 2 for a particular distributed layer 1 and sends it to the receiver. The receiver aligns the two layers and the secret information is revealed, this without the need for an encryption device, a computer or performing calculations by hand. The system is unbreakable, as long as both layers don't fall in the wrong hands. When one of both layers is intercepted it's impossible to retrieve the encrypted information.

Algorithm 2: Image Encryption

Step1: Get number of share images from user let it be N
Step2: Get Gray image height & width
Step3: Calculate the area of the image
Step4: Create N empty images objects
Step5: Divide the gray image into NxN matrix block representing the pixel as it elements for whole area.
Step6: Also divide the empty image objects into NxN matrix block representing the white pixel as it elements.
Step7: For each block in image convert NxN matrix into N column matrix
Step8: Assign each column to the each empty image object, location representing to NxN matrix column
Step9: Do this process for the each block till you covert the whole image area.

3. Watermarking Technique

In this process we will be adding a label to the share images to avoid the management issues to the UN-predictability of the noise content. This should be done without any pixel expansion problem. We are using a watermarking technique to add a cover image or a label to the share image. Initially we are getting the pixel count by getting the width and height of the share images. Adding to much pixel to another image may increase the size of the content and another point is that label need not to be as exact as it original size. So we scale the image smaller to its original size. The scaling process depends upon the image content. After scaling the image we search for white spaces and insert the cover image pixel one by one into the share images. By means of this, it's not required to remove the cover images at the decryption phase, as well as it reduces shares synchronization time. Where removing cover images results in pixel expansion problem.

Algorithm 3: Adding cover images

Step1: Get the cover image from the Users
Step2: Convert the image into gray Scale image
Step3: Get Share image height
Step4: Get Share image width
Step5: Cover image height (Hc)=Share Image Height/12;
Step6: Cover image width (Hw)=Share Image width/12;
Step7: Scale cover Image to height (Hc) and (Hw)
Step8: Get Corner location and Its area
Step9: Find the white spaces in between the pixels
Step10: Add the Cover Image pixel
Step11: Repeat the process until we finish adding all the pixel form the Cover Image.

4.Image Decryption

The decryption of the image will be done by overlapping the shares, without removing cover images, by means of that we can avoid pixel expansion problems. Where removing cover images results in change in the display quality of the recovered image. When we place both the shares one over another with proper alignment, we can interpret the original image without changing the display quality of the recovered image.

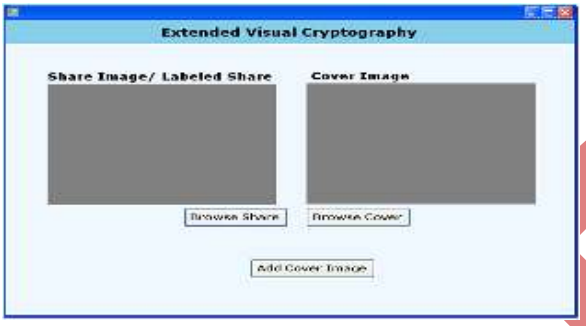
VI. EXPERIMENTAL RESULTS

In this section, we first evaluate the performance of the proposed optimization model by comparing with the previous VC results for GASs. Then, we assess the performance of the proposed Watermarking technique for EVCS in terms of the pixel expansion and some management problems. Finally, we demonstrate the results of our implementation of EVCS by examples.

Upload a secret image

Converting original image to Grayscale image

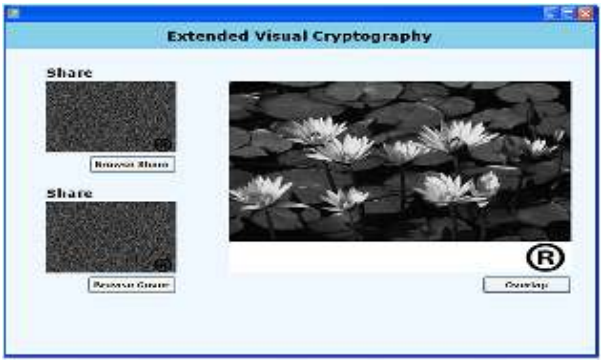
Perform encryption



Add cover images

Adding cover image to share at bottom corner

Overlapping shares



Final output

VII. CONCLUSION

In this paper, we have proposed a two-phase encryption algorithm for the EVCS for general access structures. From the pixel expansion point of view, our approach successfully solves the open questions. The display quality of the recovered image, which includes contrast, perfect reconstruction of black secret pixels, and maintenance of the same aspect ratio as that of the original secret image are preserved. Each phase in the encryption procedure is less coherent, so it can be individually designed and also can be replaced separately. The density of the cover images is adjustable, it is very helpful for modifying the display quality of the cover images.

REFERENCES

[1] M. Naor and A.Shamir, “Visual cryptography,” in Proc. Advances in Cryptology (Eurprocrypt’94), 1994, pp. 1–12.

[2] E.R.Verheul and H. C. A. v.Tilborg, “Constructions and properties of k-out-of-n visual secret sharing schemes,” Designs Codes Crypto., vol. 11, pp. 179–196, 1997.

[3] H. Koga, “A general formula of the (t,n)-threshold visual secret sharing scheme,” in Proc. Advances in Cryptology (Asiacrypt), 2002, pp. 328–345.

[4] Gamil R.S. Qaid and Sanjay N. Talbar,’’Encryption and Decryption of Digital Image Using Color signal” IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 2, March 2012

[5] C. Blundo, S. Cimato, and A. D. Santis, “Visual cryptography schemes with optimal pixel expansion,” Theor. Comput. Sci., vol. 369, pp.169–182, 2006.

[6] D. Wang, L. Zhang, N. Ma, and X. Li, “Two secret sharing schemes based on boolean operations,” Pattern Recognit., vol. 40, pp. 2776–2785, 2007.

[7] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, “Visual cryptography for general access structures,” Inform. Comput., vol. 129, pp. 86–106, 1996.

[8] C. S. Hsu, S. F. Tu, and Y. C. Hou, “An optimization model for visual cryptography schemes with unexpanded shares,” Found. Intelligent Syst., LNAI, vol. 4203, pp. 58–67, 2006.

[9] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, “Extended capabilities for visual cryptography,” Theor. Comput. Sci., vol. 250, pp. 143–161, 2001.

[10] F. Liu, C. Wu, and X. Lin, “Step construction of visual cryptography schemes,” IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 27–38, Mar. 2010.