ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 1, Issue 9, November 2012

Resultant Variant Cryptography by using Morphological Transformation Domain for Google Maps

C.Veerabhadra Rao, G.Gayatri

Abstract— **Visual Cryptography is a cryptographic technique which can hide the visual data (images, pictures, text etc.) and which can be decrypted without a computer but in a tedious way. The best-known techniques that visual cryptography has are encrypting the images by breaking those images into n shares. Each n-1 share will not reveal the actual image but decrypting the n shares will give the actual information of the image. We can also make the image zoom and find out the information in it but we can hide this information through these techniques of visual cryptography. Even Watermarking is one of the beautiful techniques which protect the copyright ownership of a digital image. According to the proposed method, the watermark pattern does not have to be embedded into the original image directly, which makes it harder to detect or recover from the marked image in an illegal way. It can be retrieved from the marked image without making comparison with the original image. However, their concepts are different but their main purpose is of hiding the original information. For visual cryptography, a set of share binary images is used to protect the content of the hidden image. The hidden image can only be revealed when enough share images are obtained. For watermarking, the hidden image is usually embedded in a single halftone image while preserving the quality of the watermarked halftone image. Hence, visual cryptography requires no understanding and, because security is effectively in the hands of the end user, he or she has a feeling of control, which promotes trust.**

I. INTRODUCTION

Our motivation for this type of viewing is the resultant variant cryptography by using morphological transformation domain for Google maps. As the user increases the zoom level the watermark can be visible within the images. The same here in this paper, when the image is zoomed out no watermark can be identified and further the zoom level increases the watermark can be viewed. We present an example (figure 1) of censoring and watermarking technique. Which shows figure 1(A) an example of watermarking feature, figure 1(B) an example of representing a drawing of facial blurring technique, 1(C) an example of a picture of the license plate censoring technique.

As we know that the visual cryptography is a technique to hide information in images. This visual cryptography provides two types of transparent images that one image contains the secret information and the other contains random pixels. By using this visual cryptography shares, the visual cryptography scheme effort to do a conjunction of zooming images to recover secure secret information. Additionally, we discuss about the potential application for content based visual cryptography. In visual cryptography the existing techniques are encrypting the full image. In order to hide particular information, the content based scheme aspects are used. By using this visual cryptography the data can be recovered.

Fig1 (a) watermarking technique, (b) facial blurring technique, (c) license plate blurring technique.

A. Visual cryptography security and properties

Today security is very important in visual cryptography. As we know that many issues are emerged due to public information. A very prominent issue is to protect the personal private aspects from the public users. In visual cryptography, the personal private information can be recovered by using a specific chunk of information. Here concurrently the information keeps private from public users. From the original image a random permutation of pixel patterns are selected to represent white and black pixels. , it is difficult to know that the corresponding shares

contain the same or complementary pixel patterns when shares are separate. This makes complex to determine the secret based on cryptographic analysis of a single share Visual Cryptography is a very impressive and successful technique. Visual cryptography has a very attractive properties, it is very desirable in the form of secret sharing as well as authentication. Which integrates both the notion of perfect ciphers [1] and the secret sharing in VC? Particularly, in secret sharing visual cryptography the binary images are used. A binary images can be split into number of n chunks (shares) where k or more of those chunks (k<_n), which can be stacked together, inexactly recover the actual image. Therefore (k, n) is a secret sharing.

The usage of visual cryptography is very easy. Secret recovery is as simple as stacking each share. In order to decrypt the share there is no computation required. In Visual Cryptography scheme, the contrast of the recovered secret is also very important. The contrast should be as optimal (high) as possible [7]. By the above properties we can define a good visual cryptography scheme. For designing a new scheme for secret sharing, the above properties must be considered carefully. The purpose of new visual cryptography that allows the user to repeatedly hide many secrets in a elevated resolution image. We can use designed shares to implement the idea of multiple secret recovery at multiple resolutions. By combining the binary chunks (shares) with the colored images from visual cryptography that are used within the Google Maps. In the image, secret chunks have to be inserted. After the insertion completed, to recover the image to the exact chunks has to be used. When the image is zoomed out, it reveals the next level secrets.

II. EXISTING SYSTEM

The topic of recursively hiding secrets within a set of shares has been extensively researched [9] [10]. The scheme proposed in applies [9] to images and text and attempts to increase the efficiency of traditional VC to make it possible to hide extra secret information that serves as steganographic channel. The scheme involves recursive hiding of smaller secrets within a larger secret. Each step involves doubling the secret size, thereby increasing the information that every bit of share conveys to (n-1)=n bits of the secret. However, this method is not threshold based, as every share is required to fully reconstruct the secrets. A recursive approach to space efficient visual cryptography has also been taken into consideration [10]. The recursive approach to space efficient secret sharing presents a technique that distributes k-1 secrets of length b each into n shares such that each share if effectively of length n /k-1 .b and any k pieces can be used for the secret reconstruction. The scheme is near efficient since n/k-1 is near the optimal factor n/k which can be chosen to be close to one. This work is based on computational models for secret sharing in which a symmetric key is used to encrypt the original secret. It is obvious from the previous work that many thoughts have been given to the idea of recursive information hiding within visual cryptography. However, the idea of embedding these types of recursive shares within a high resolution image for the purpose of zoomed secret recovery, to our knowledge, has never been considered.

III. PROPOSED SYSTEM

In this paper we can propose three main contributions. The first one deal with embedding visual cryptography shares within the license plate location .The second involves creating a recursive multiple resolution visual cryptography scheme and the third includes swaps the pixels 3*3 and 2*2 in a related secret image [8].

A. License Plate Embedding

Due to restricted issues the adjacent location of Google maps and its street view implementation, provide some information of Google censor. However, we are not familiar whether the original images are kept. Here our plan for embedding a visual cryptography share, the blurred region allowed to include the original image consist the un blurred license plate. i.e., the authenticated users only can access the license plates. In visual cryptography scheme (2, 2) has been introduced. The (3, 3) or (4, 4) schemes forms are to be used. In order to get the data they are three or four authenticated users to be extant, while recovering the license plate aspects. A total set of authenticated shares would be required to takes very complex to obtain. In addition the scheme security as applied to prevent the copied image [11]. Many techniques are accessible which help in identifying and detecting license plates. In this kind of application, the automatic license plate recognition (ALPR) technique is also used [12] [13]. We can determine the license plate by using this automatic proposed system. However, this system works very effective with a large range of license plates [13].

In order to blur the identification number, a Gaussian blur effect is used to determine the license plate and recorded the license number identification. When we are looking the final blurred image the unknown user cannot recognize the identification number. Now we can replace the represent Gaussian blur in required location 21*21 with pixel blurring filter. This allows adequate blurring, which removes an important point of the license plate and rendering it unreadable. The advantage of this blurring technique is embedding in a visual cryptography share. In blurred location, the alterations or changes cannot be reducing the image quality and can also add some extra data in a perfect location. Using this ALPR, we can determine the license plate along with determining the license plate identification number. After determining the identification, we can create an image in an appropriate size that contains an identification number. Now we can

use this image as visual cryptography secret which generates two shares. Due to this multi-purpose usage of visual cryptography, it is possible to create a set of shares such as two or more users can retrieve the license plate.

B. Multi-resolution VC Scheme

In multi-resolution visual cryptography scheme, within the Google Street View the watermarking technique is used. Here the scheme works as, the smallest secret is determined and a (2, 2) set of shares are created. We notate S_1^1 and $S2^1$ shares are used. Here share one based on one secret and share two based on another secret. By using these shares, each share can generate the larger shares of the next secret. This is known as the recursive part of the scheme. First, we create these shares to determine the ratio. This allocates to create the next set of shares. Here the original secrets of sizes are 128*128, 256*256, and 512*512. Then the secret one contains four images as that embed into secret two, the embedded four images of secret two again embedded into secret three and so on. Here the ratio is 14.Now the first set of shares of secret one is generated. Then the two new images N1 and N2 construct, which will be the new set of shares. This two new images can placed in the earlier created shares. So the two new images are share one and share two of secret two. This can be represented as $S1^2$ and $S2^2$. Then the two new images can be split into different quadrants, N^1q1;:::; q4 and N^2 q1;:::; q4 . : The four quadrants as the same size that are generated and they can be expresses as:

$$N^1 = \begin{bmatrix} q1 & q2 \\ q3 & q4 \end{bmatrix} and\ N^2 \begin{bmatrix} q1 & q2 \\ q3 & q4 \end{bmatrix} \qquad (1)$$

The new shares S_1^2 and $S2^2$ are follows: S_1^1 is placed into q1 of N1, $S2^1$ is placed into q4 of N2.as we know that the second secret is ready, then the remaining quadrants can randomly generate for every new images. The results of new images can generate as follows:

$$S1^1 = \begin{bmatrix} S_{1^1} & R2 \\ R3 & R4 \end{bmatrix} and\ S2^2 \begin{bmatrix} R1 & R2 \\ R3 & S2^1 \end{bmatrix} \qquad (2)$$

Where R1,.... 4 represents the randomly generated share. By using similar recursive steps, this process can be repeated for any remaining secret as shown in the fig 2.

C. Swapping

In this block size is constrained by 3* 3 pixels or larger; we process an image in 2* 2 pixel blocks. This allows flexibility in tracking the edges and also achieves low computational complexity. The two processing cases that flipping the candidates of one does not affect the flip ability conditions of another are employed for orthogonal embedding, which renders more suitable candidates can be identified such that a larger capacity can be achieved.

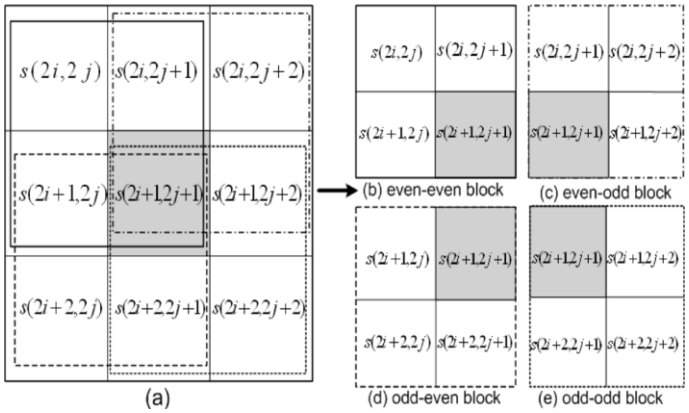
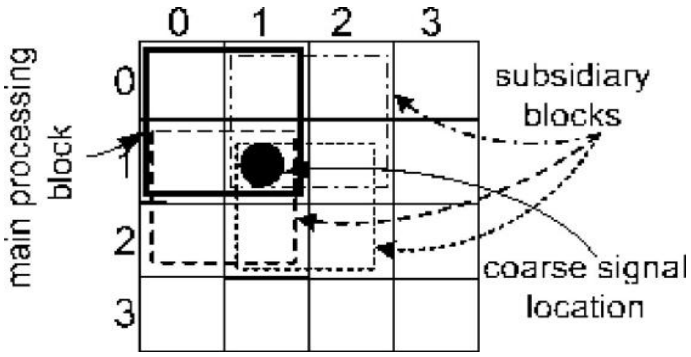


Figure 2 Four different 2 *2 blocks in a 3 *3 block of a binary image.

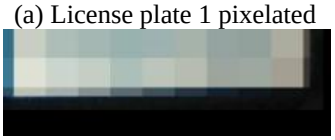
In the above diagram the image is divided into 3*3 blocks. Again each block is divided into 4 2*2 blocks. Those are: These blocks are given below: 1.even-even block, 2.even-odd block, 3.odd-even block, 4.odd-odd block. In each block we follow the following process as shown in below.



IV. EXPERIMENTAL RESULTS

An example of license plate blurring or filtering can be viewed is shown in the figure. By using these visual cryptography techniques, from the results it is very clear that can be removed the license plate details. The results of new recursive secret sharing scheme can be viewed. Here within the set of shares, there are three secrets has been hidden. When the second share is shift to left, the second hidden secret can be viewed. While this process is repeated the original small secret can be obtained.

(a) License plate 1 pixelated



. (b) License plate 2 pixelated

(c) License plate 1 VC

(d) License plate 2 VC

. (e) License plate 1 recovered.

(f) License plate

Figure 4 Obscuring license plates and accurately recovering them were using VC.

V. CONCLUSION

From these results, it is clear that visual cryptography could be used to obscure personally identifiable data from Google Street View The added benefit of using visual cryptography rather than typical blurring techniques is that it would be possible to recover these details.

This allows the original unblurred images to be removed and only those who possess the appropriate combination of visual cryptography shares can recover the secret information. We chose the ratio of 1/4 initially for our testing. Further development is required to address arbitrary ratios with the overall goal of obtaining the optimal solution using these techniques.

The other benefit is that these images may be publicly uploaded with the embedded visual cryptography share. This would guarantee global access to the encrypted information, for those who are authorized to recover it. Additionally, combining smaller secrets within a set of shares has a useful application within the likes of Google Maps. The recovered secrets may be smaller, but this becomes irrelevant after the image has been suitably zoomed.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptology- Eurocrypt '94, vol. 950, pp. 1 – 12, 1994.
[2] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, "Extended schemes for visual cryptography," Theoretical Computer Science, vol. 250, pp. 1 – 16, June 1996.
[3] Z. Zhou, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography,"IEEE Transactions on Image Processing, vol. 15, no. 8, pp. 2441– 2453, Aug. 2006.
[4] J. Duo, W. Yan, and M. S. Kankanhalli, "Progressive color visual cryptography," SPIE Journal of Electronic Imaging, vol. 14, no. 3, 2005.
[5] J. Weir and W. Yan, "Image hatching for visual cryptography," in 13th International Machine Vision and Image Processing Conference, 2009.IMVIP '09, September 2009, pp. 59–64.
[6] J. Weir and W.-Q. Yan, "Sharing multiple secrets using visual cryptography,"in IEEE International Symposium on Circuits and Systems, 2009.ISCAS 2009, May 2009, pp. 509–512.
[7] C. Blundo, P. D'Arco, A. D. Santis, and D. R. Stinson, "Contrast optimal threshold visual cryptography schemes," SIAM Journal on Discrete Mathematics, vol. 16, no. 2, pp. 224–261, 2003.
[8] J. Weir, W. Yan, and D. Crookes, "Secure mask for color image hiding,"in Third International Conference on Communications and Networkingin China, 2008. ChinaCom 2008, Aug. 2008, pp. 1304–1307.
[9] M. Gnanaguruparan and S. Kak, "Recursive hiding of secrets in visual cryptography," Cryptologia, vol. 26, no. 1, pp. 68–76, 2002.
[10] A. Parakh and S. Kak, "Space efficient secret sharing: A recursive approach," 2009. [Online]. Available: http://www.citebase.org/abstract?id=oai:arXiv.org:0901.4814
[11] J. Weir and W.-Q. Yan, "Dot-size variant visual cryptography," in IWDW '09: Proceedings of the 8th International Workshop on Digital Watermarking. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 136–148.
[12] S.-L. Chang, L.-S. Chen, Y.-C. Chung, and S.-W. Chen, "Automatic license plate recognition," IEEE Transactions on Intelligent Transportation Systems, vol. 5, no. 1, pp. 42–53, March 2004.
[13] D. Zheng, Y. Zhao, and J. Wang, "An efficient method of license platelocation," Pattern Recognition Letters, vol. 26, no. 15, pp. 2431–2438,2005.

C.Veerabhadra Rao is Associate Professor of Computer Science department at MVGR College of Engineering, Viziangaram(AP).
G.Gayatri is currently a M.Tech student of Computer Science department at MVGR College of Engineering, Viziangaram(AP).