ISSN:0975-9646

A secured Transmission of Embedded Hidden Data in Binary Images Using Resolution Variant Visual Cryptography

Koppala K V P Sekhar, S Sateesh Kumar, Y.Ramesh Kumar

CSE Department, Avanthi College of Engg & Tech,
Cherukupalli, Vizyanagaram,Andhrapradesh,India.

Abstract: Resolution variant visual cryptography takes the idea of using a single share of visual cryptography (VC) to recover a secret from an image at multiple resolutions. That means, viewing the image on a one-to-one basis and superimposing the share will recover the secret. However, if the image is zoomed, using that same share we can recover other secrets at different levels. The same share is used at these varying resolutions in order to recover a large amount of hidden secrets. This process is quite similar to watermarking an image, whereby nothing can be seen while fully zoomed out, but as the zoom level is increased the watermark becomes visible. This would also be associated with a recursive style of secret sharing. This type of secret sharing scheme would be appropriate for recovering specific types of censored information, such as vehicle registration numbers within certain types of images. This adds an additional dimension to our scheme: content based visual cryptography. This schema is used for only for bitmap images. We decode the original image into two images and transfer data to the secured manner by using any cryptography techniques. we integrate those two images then we get original image.

INTRODUCTION:

Our motivation for this type of resolution variant secret sharing scheme stems from the idea used within Google Maps Street View. As the reader may be aware, when fully zoomed out within the interactive Google Maps application, no watermarks can be viewed. However, as the user increases the zoom level visible watermarks can be identified within the images. The same is true for the Street View implementation which further increases the zoom level. It provides an example of this type of censoring and watermarking technique. The watermarks are only slightly visible. As the zoom level is increased, they become more prominent. Our resolution variant visual cryptography scheme attempts to use this idea of zooming in conjunction with secure secret recovery using VC shares. Additionally, we explore the potential application for content based visual cryptography. Current techniques within visual cryptography look at encrypting the full image. Our content based scheme looks at specific sections of an image in order to hide certain data. This data can be recovered using visual cryptography.

Many issues surround this type of publicly available information. It is highly important that personal private details that could potentially identify someone are kept hidden from the public. In some cases, these pieces of information may be required by specific agencies, such as law enforcement. In these cases, visual cryptography can be used to recover the specific pieces of information, while simultaneously keeping the information private from public viewing. Visual cryptography is a very efficient and effective form of secret sharing. It combines the idea of secret sharing with the notions of perfect ciphers. Typically, binary images are used within this type of secret sharing. A single secret image is split into a number of n pieces (known as shares) where any k or more of those shares (k, n), when physically stacked or superimposed, approximately recover the secret image. This is known as (k; n) secret sharing.

There has been a lot of research within the field of visual cryptography. From extended schemes, whereby the shares contain meaningful information, to schemes which involve natural looking images which use grayscale, color and even image hatching techniques. Sharing multiple secrets within a set of shares has also been considered. Visual cryptography itself has a number of very attractive properties which make it very desirable as a form of secret sharing or even as a form of authentication. VC is very easy to use. Secret recovery is as simple as stacking each share. No computation is required in order to decrypt the shares, the decryption is also instantaneous.

Another important aspect of any VC scheme is the contrast of the recovered secret. The contrast should be as optimal (high) as possible. Security is also very important. Given a secret, a random permutation of pixel patterns is chosen to represent white and black pixels from the original image. When the shares are separate, it is impossible to tell whether the corresponding shares contain the same or complementary pixel patterns. This makes it difficult to determine the secret based on cryptographic analysis of a single share.

With these properties in mind, we can define a good base for a new VC scheme. These properties should be taken into consideration when designing any new scheme for secret sharing. Within this paper, we propose a new VC scheme that allows the user to recursively hide many secrets within a high resolution image. We use specially crafted shares to support the idea of multiple secret recoveries at multiple resolutions. The ideas presented in are employed to combine the binary shares from visual cryptography with the color images used within Google Maps. After the secret has been embedded within the image, its corresponding share can be used to recover the image. As the image is zoomed on screen, superimposing the share again reveals the next level of secrets.

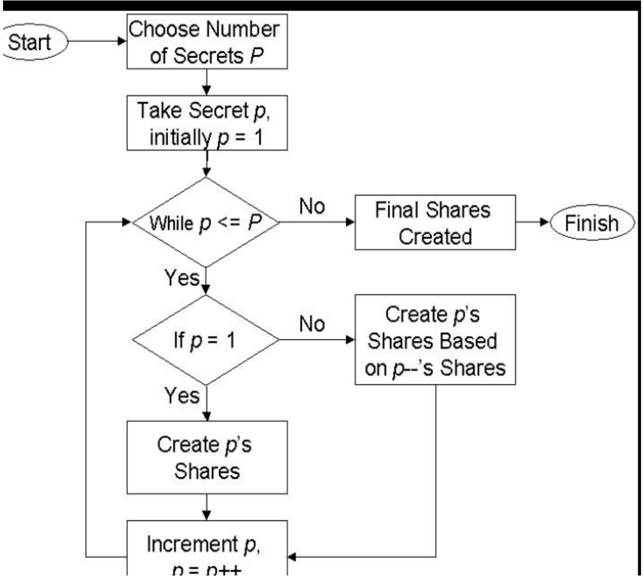
Due to privacy issues surrounding Google Maps and its Street View implementation, Google censor some information. However, it is not known whether the original images are kept. Our scheme for embedding a VC share within this blurred region would allow for the original image containing the un-blurred license plate to be deleted from their system. This means that the only people who are approved to access the license plates are the people with the corresponding share(s), i.e. authorized users.

As a proof of concept we introduced our ideas as a (2, 2) visual cryptography scheme. In practice, a stricter form of VC scheme would be used. For example, a (3,3) or (4,4) scheme. This would require three or four authorized users respectively to be present when recovering license plate details. Even if copies are made, a complete set of authorized shares would be required which may prove more difficult to obtain. To further the security of the scheme, an adaption could be applied to the shares in order to prevent copying. Many techniques are available which assist in locating and detecting license plates. The automatic license plate recognition (ALPR) technique would be most appropriate for our type of application. Using the system proposed, we can automatically determine which characters make up the plate. Some false positives do occur however, although this system works very well with a very wide range of license plates.

After the license plate area has been determined and the license number identification has been recorded, a Gaussian blur effect would typically be used within this area in order to obscure the identification number. When viewing the final images after blurring, it is clear that the identification numbers are unrecognizable. We replace the typical Gaussian blur with a pixilated blur filter with an area of 21 _ 21. This provides sufficient blurring which removes the salient points of the license plate, rendering it unreadable.

Our scheme takes advantage of this blurring technique by embedding a VC share within this area. As the area is already blurred, making any changes to it will not reduce the overall image quality and presents a perfect location to add some extra data. Our scheme works as follows: Using ALPR, we can determine the size of the area that contains the license plate along with determining the license plate identification number. After determining the identification, we can create an image of the appropriate size (based on the size of the area to be blurred) which contains this identification number. We then use this image as the VC secret, generate two shares and embed share one within the license plate region. Due to the versatile nature of VC, it is possible to create a set of shares such that two or more people must be present in order to recover the license plate number. This also makes it more difficult for assailants to recover the license plate data for their own personal use.

The below figure shows our mechanism:



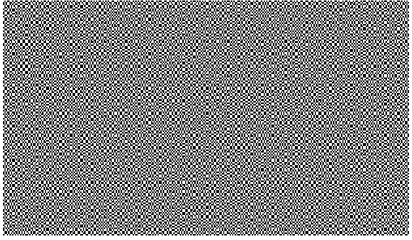
Operations:

Initial image: initially we are taken the following image

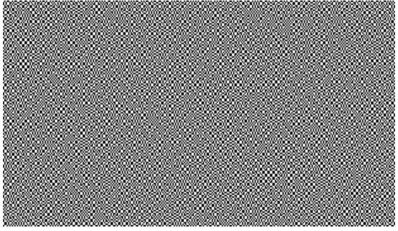
After processing:

We divide the images into two as shown in below

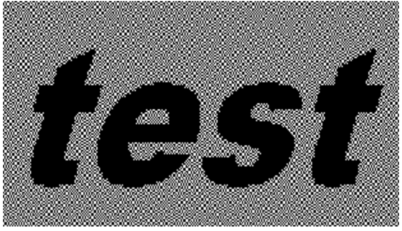
First image:



Second image:



After integration:



CONCLUSION:

From these results, it is clear that VC could be used to obscure personally identifiable data from Google Street View. The added benefit of using VC rather than typical blurring techniques is that it would be possible to recover these details. This allows the original un-blurred images to be removed and only those who possess the appropriate combination of VC shares can recover the secret information. We chose the ratio of 14 initially for our testing. Further development is required to address arbitrary ratios with the overall goal of obtaining the optimal solution using these techniques.

It provides security for data placed or embedded in the images. We can use this one for certificates and secured data transmission.

REFERENCES:

[1] Resolution Variant Visual Cryptography for Street View of Google Maps by Jonathan and WeiQi Yan,Weir,Queen's University Belfast,Belfast, BT7 1NN

[2] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptology - Eurocrypt '94, vol. 950, pp. 1 – 12, 1994.

[3] 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.

[4] 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.

[5] J. Duo, W. Yan, and M. S. Kankanhalli, "Progressive color visual cryptography," SPIE Journal of Electronic Imaging, vol. 14, no. 3, 2005.

[6] 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.

[7] 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.

[8] 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.

[9] J. Weir, W. Yan, and D. Crookes, "Secure mask for color image hiding,"in Third International Conference on Communications and Networking in China, 2008. ChinaCom 2008, Aug. 2008, pp. 1304–1307.

[10] M. Gnanaguruparan and S. Kak, "Recursive hiding of secrets in visual cryptography," Cryptologia, vol. 26, no. 1, pp. 68–76, 2002.

[11] 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

[12] 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.

[13] 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.

[14] D. Zheng, Y. Zhao, and J. Wang, "An efficient method of license plate location," Pattern Recognition Letters, vol. 26, no. 15, pp. 2431–2438, 2005.