International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

A Quality Maintain Visual Cryptography Scheme

Anju G

M.Tech Student, Dept. of Computer Science and Engineering, M.G University, Mount Zion College of Engineering, Kadammanitta, Pathanamthitta, Kerala, India

Abstract: ***Visual cryptography is a cryptographic scheme that focuses on solving the problem of secret sharing of data which hides in images. The multi-secret visual cryptography (MVC) scheme is capable of sharing multiple secret images. Like this, the tagged visual cryptography (TVC) scheme hides tag images in randomly selected shares. But these cryptography schemes creates distortions in the shares at the time of encoding. Due to this, occurs a reduction in the quality of image at the time of decoding. So, this scheme introduces an extended TVC called Lossless tagged visual cryptography (LTVC) scheme where the encoding will not affect the quality of the rebuilt secret image, i.e., the decoder can rebuild exactly the identical image. Here also introduces a probabilistic LTVC (P-LTVC) to overcome the security issues.***

Keywords: Visual Cryptography, Visual Secret Sharing

1. Introduction

The security of data is one of the most important issue we want to focus. The visual cryptography proposed by Naor and Shamir is a technique that allows information such as images, diagrams or text to be encrypted using an encoding system that can be decrypted by human visual system. It doesn't require a computer to decode.

A (k, n) VC scheme encodes a secret image into 'n' noise like shares (called transparencies or shadows). When k or more shares are superimposed together, we can retrieve the secret image. Any less than k share discloses no information of the secret image. VC becomes a reliable technique for the applications where the decoding are not available or too costly. The VC can be extended to multi-secret visual cryptography (MVC) scheme for hiding more information in the encoding process. After, Wang and Hsu proposed a tagged VC (TVC) scheme where more information can be revealed by folding up operation. In this we can fold up a share along its midline, an additional secret image is visually presented.

However, the main problem of both MVC and TVC is that they cause distortion to the shares of conventional VC. Also the decoded secret image in these schemes has lower quality than that of the conventional VC. To overcome this problem, this paper proposes a lossless tagged visual cryptography (LTVC) scheme which hides multiple secret imaged without affecting the quality of the original secret image. As a result the decoder can rebuild exactly the same image as that of the conventional VC. The experimental results illustrate that stacking results of LTVC has higher contrast than that of other tagged visual cryptography method. And also as compared with the other multi secret visual cryptographic scheme the Lossless Tagged Visual Cryptography gives better quality to the decoded secret image.

The remaining of this paper is organized as follows: Section 2 describes the background study and 3 provide a brief methodology, and the proposed LTVC method. We then present the result analysis in Section 4 and discuss some implementation details.. We conclude the paper in Section5.

2. Background Study

The proposed scheme uses Naor and Shamir's VC technique to encode the secret images into several shares, and by adjusting the pixels, tag images can be hides to these shares. In this section describes the Naor and Shamir's VC construction method.

In the conventional (k, k) LTVC scheme a ground set G is first defined. The ground set G has 2^k different subsets .Then $G-even$ denotes the collection of all the subsets of even elements and the $G-odd$ denotes the collection of odd elements. After that two matrices are generated, one contain white pixels and one contain black pixels. The colums of white pixel are permuted when the sharing of white pixel. And each row of the permuted results corresponds to the sub pixels in each of the k shares. Due to this construction, it will satisfy all the security and contrast conditions. Then restricts a $k \times 2^{(k-1)}$ matrix to a $(k-1)\times 2^{(k-1)}$ matrix by deleting a row in all possible way, then we get collection of matrices.

3. Proposed Method

In the proposed method (k, k) LTVC scheme is introduced. In this the encoding process used is same as that of the conventional visual cryptographic method. The (k, n) LTVC scheme first shares the secret image S into n shares. We can reveal secret image when k or more shares are superimposed together. Any less than k shares discloses no information of the secret image. Using the folding up operation, the (k, n) LTVC scheme can have the ability to disclose several tag images.

The proposed LTVC scheme include a secret image S and several tag images. The output of the (k, k) LTVC scheme is the k shares. We can visually recover the secret image when stacking together the k shares. And the k-1 of k shares can disclose k-1 tag images by using the folding up operation.

For this consider a folded up pair S(x, y) and S(x, y'). In the conventional visual cryptographic method, the encoding of these two pixels is carried out independently. While in the

case of LTVC the S(x, y) is shares using the conventional VC technique. The S(x, y') is encodes according to the shares of S(x, y). In this $_2{}^{k-1}$ subpixels are generated for each pixel in the secret image S.

Here we consider the first k-1 shares to embed the tag images. These k-1 share collection generates $(k-1)\times 2^{(k-1)}$ matrix M. Each row in M includes one share of the secret image S(x, y). If S(x, y) == 0 , the M belongs to C^0 and if S(x, y) == 1, the M belongs to C^1. Then a vector is produced by sequentially collecting the pixels in the k-1 tag images. The colums of M are then possible combinations of k-1 tag images. So there is a colum in M which is exactly identical with the vector. We can denote this colum as $M(:, C^{tag})$. In the Matrix M there will be black and white colums. We can define the black colum as C^{black} and white colum as C^{white}. Then we construct construct a matrix M'. It is constructed to represent the first k-1 shares of S(x, y), and the function FOLD (y) = $_2{}^{k-1}$-y+1 returns the colum position of M' which stacks together with y th colum of M after the folding operation.

Then analyze the light transmission of the tag images. When folding up the share images of M and M' and are stacked together , compute stacked vector. If the tag image is zero, the stacked vector have two white pixel. If the tag image value is 1, the the stacked vector consist of only black pixel. So the contrast of the tag image is greater.

The first k-1 shares of S(x, y) are constructed according to M'. Each share in in the image is corresponds to one row of M'. Finally, construct the last share of S(x, y).

The LTVC constructs the secret image's sub pixel S(x,y') according to the shares of conventional visual cryptography. Collecting the k shares of S(x, y) according to S(x, y') forms a $k \times 2^{(k-1)}$ matrix N When the S(x, y)==S(x, y') , each colum of N can find a complimentary colum in N' of order (x,y'). Then we can easily identify that these two colums are same, but the colums are distributed in different locations. The shares generated using the LTVC technique will be satisfy the security and contrast conditions.

We can extend the proposed LTVC technnique to Droste's (k, n) VC scheme where the embedding the tag images are same as that of the LTVC.

3.1 Discussion of Security and P-LTVC

In this section we develop a probabilistic LTVC for improving the security of the LTVC. In this P-LTVC also constructs a matrix, where the colum in M' is randomly selected colum from the M and it will not repeat with any other colums of M. Here the vector is obtained by selecting 1 of k-1 elements and applying the complement operation to this element with 50% probability. Here also ensure that folding up the last share does not reveal the information of tag images.

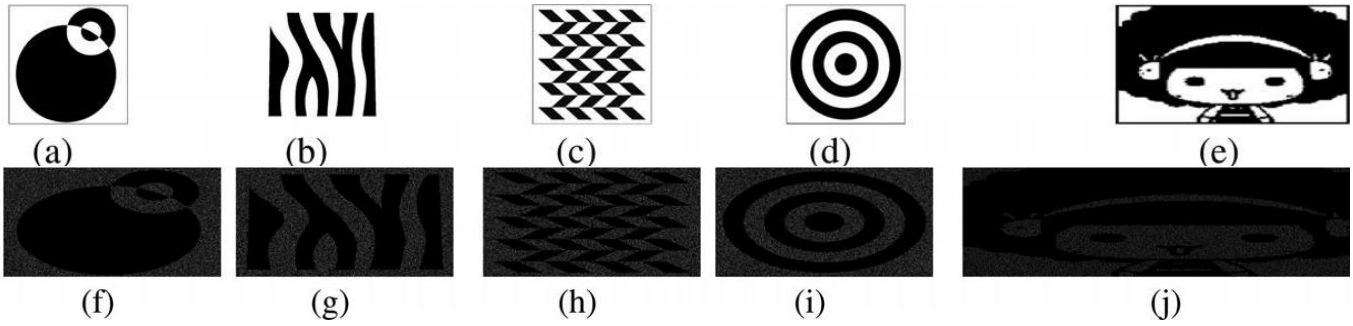
We then calculate the light transmission of P-LTVC technique. If the tag pixel= white, C^{white} =0 and C^{tag} =0 .But we cannot determine the pixel values of other pixels because the corresponding colums are selected randomly. From this understood that the contrast of the tag images i worse as compared to LTVC.

4. Result Analysis and Discussion

In this section a comparison is carried between the Wang et al,'s TVC scheme and the proposed LTVC and P-LTVC for evaluating the performance. For this, one binary cartoon image is used as the secret image Fig.1 e and four binary images are used as the tag images (Fig. 1(a),1 (b),1(c),1(d)). The results of (4,4) TVC, LTVC and P-LTVC is respectively shown in Fig.1.The decoded tag images and secret image is included in the result.

LTVC scheme provides best performance in contrast on both tag images and secret image. Therefore the decoded images of the LTVC scheme has higher visual quality as compared to the other schemes.

In the case of LTVC, when the k < 6 the LTVC produces better tag images than TVC. But when k > 6 the TVC produces better tag images than the LTVC. The P-LTVC schems is more better when considering the contrast and security than LTVC.
One drawback of the LTVC and P-LTVC is that we can encrypt less information than the TVC. The (k, k) TVC is able to encrypt k tag images, whereas the (k, k) LTVC and (k, k) P-LTVC can encrypt only k-1 tag images.



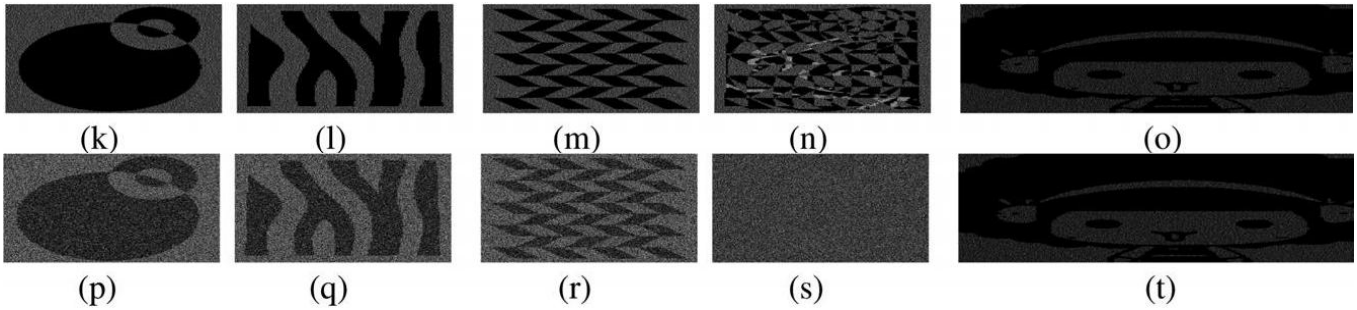


Figure 1: . Performance comparison between (4, 4)-TVC, (4, 4)-LTVC and (4, 4)- P-LTVC. (a) -(d) are tag images, and (e) is secret image. (f)-(i), (k)-(n) and (p)-(s) are decoded tag images of TVC, LTVC and P-LTVC, respectively. (j), (o) and (t) are decoded secret images of TVC, LTVC and P-LTVC, respectively.

5. Conclusion

Based on conventional VC, here proposed a lossless tagged multi secret visual cryptography (LTVC) scheme. This (k, k) LTVC scheme can add additional k-1 tag images and secret image. When superimposing the k shares , we can recover the secret image. Then tag images are retrieved by folding up the k-1 shares. As compared with the other multi secret visual cryptographic scheme, the embedding of tag images does not lower the quality of the secret image. The proposed LTVC scheme has higher contrast than that of the other cryptographic method.

References

[1] R.-Z. Wang and S.-F. Hsu, "Tagged visual cryptography," IEEE Signal Process. Lett., vol. 18, no. 11, pp. 627–630, 2011.
[2] M. Naor and A. Shamir, "Visual cryptography," in Advances in Cryp-tology–EUROCRYPT 1994, ser. Lecture Notes in Computer Science, A. De Santis, Ed. Berlin/Heidelberg, Germany: Springer, 1995, vol. 950, pp. 1–12.
[3] C. Wu and L. Chen, "A study on visual cryptography," Master Thesis, Inst. Comput. Inf. Sci., National Chiao Tung Univ., Hsinchu, Taiwan, 1998, R.O.C..
[4] J.-B. Feng, H.-C. Wu, C.-S. Tsai, Y.-F. Chang, and Y.-P. Chu, "Visual secret sharing for multiple secrets," Patt. Recognit., vol. 41, no. 12, pp. 3572–3581, 2008.
[5] S.-J. Shyu and K. Chen, "Visual multiple secret sharing based upon turning and flipping," Inf. Sci., vol. 181, no. 15, pp. 3246–3266, Aug. 2011.

Author Profile

Anju G – M-Tech scholar in Mount Zion College Of Engineering.