Cryptographic Techniques Using extracts undisclosed Image

K.Thamaraiselvi[1], K.Dineshkumar[2],A.Mummoorthy[3]
Assistant Professor[1,2,3], Department of CSE[1,2,3], K.S.R college of Engineering[1,2,3], Tiruchengode.

***Abstract* – Modern world visual cryptographic techniques is used for data hiding and other specific scenario's, uses the characteristics of normal encryption and decryption levels of many digital images[11]. Generally, technology that uses images needs neither cryptography knowledge nor complex computation techniques. For that also it assures that cyberpunks cannot perceive any idea about the visual image in which the information is hidden[9]. The use of cryptography mainly targets binary images(BPCS) because by using the basic level of image i.e., using binary image (black & white) only we can the technique of cryptography; This piece of cryptogram proposes three sub sects for visual cryptography (VC) based on binary i.e., black and white images of gray-level and color images. There are many methods such as halftone, Visual Cryptography, etc. Many of techniques use noise-like random pixels on shares to hide secret images.**

Keywords: **Cryptography, Encryption, Half tone technique, Pixel Classification & Expansion.**

1. INTRODUCTION

It is familiar to everyone now to transfer multimedia data via Bluetooth, Zigbee, Intranet, Internet and other connectivity options. Due to the development in recent of technology, there is an importance to solve the inconvenience of assuring data security that may contain image, audio file or any other personal data which is very common to network now. There are many encrypting techniques [13] of the day-to-day life used cryptography which is usually used to protect our personal information with a high concern to secure the same.

The signal or datum which undergoes these recent trends becomes disturbed or dislocated after being done some security techniques and then is recovered by some key generation. Visual cryptography (VC) [1], [6], allows the encryption of secret information in an imageform. By applying the concept of secret sharing, a secret image can be made which is called as encrypted image. Simultaneously, anyone can share information which is quite relevant to the secret image.

VC is a very good solution for sharing secrets when computers cannot be employed for the decryption process. It consists of generation of shares using any basic visual cryptography model. In our proposed scheme, a (n, n) VC share creation is performed. Many scientists and researchers proposed new cryptography techniques, specifically in visual cryptography, by the decade of 1990's. Most of them, however, have concentrated on discussing black-and-white images, and just few of them have proposed methods for processing gray-level and color images.

The important feature of this idea is that it can reconstruct the same secret image without any further level of calculations. Its efforts put the visual system of us to read the secret messages from some overlapping shares, thus get over the drawbacks of computation that has more difficulties that require the conventional method of cryptography.

The threshold fixing method [6] makes the use of visual cryptography more flexible. If any type of their transparencies is there together, the hidden data in the secret image will be leaked and they can be mentioned as the possibility of error. If the transparency count is less than the value of threshold, the hidden data along with the cover image which can be said as the stego image or crypto image will remain hidden. A new research says that, each pixel of the color arranged pixels, which is said to be a pattern of image, is expanded into an n*n block to form two or more data sharing images.

Each n*n block on the sharing image is with the mixture of color [16] such as red, green, blue and white (transparent), etc., respectively, thus no clue about the secret image which can be diagnosed from any one of these two alone.

2. SYSTEM MODEL

Visual Cryptographic Encryption:

In the existing system, it is mandatory to do visual cryptography encryption. Without the correct key, the encrypted source content can hardly be detected even though unauthorized persons steal the data. Each pixel in the secret image is broken into four sub pixels. A white pixel is shared into two identical blocks of any number of sub pixels. A black pixel is shared into two successive blocks of 'n' sub pixels. All the pixels in the secret image are encrypted similarly using this scheme.

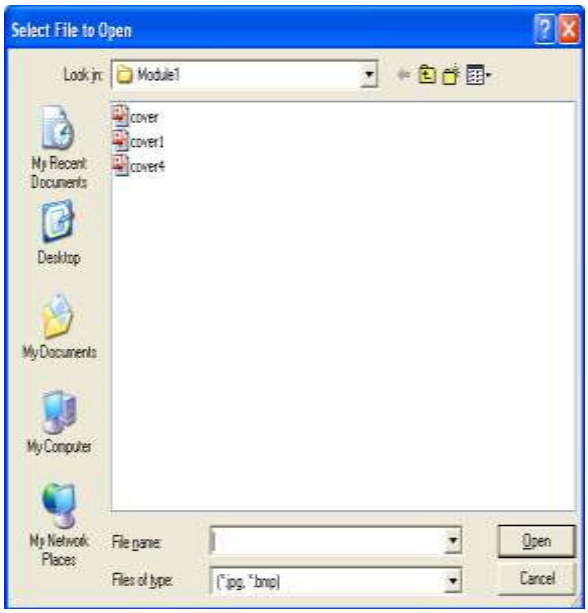

fig 1: Browsing & Selecting an image

The shares can be either Vertical, Horizontal or Diagonal shares. Any single share is a random choice of two black and two white sub pixels, which looks medium grey.

When two shares are piled together, the result is either medium grey (which represents white) or completely black (which represents black). In this phase the binary watermarked contributions extracted from the cover image. The proposed watermarking technique doesn't require the cover image or any of its characteristics for the extraction of watermark, and hence the proposed scheme is said to be invisible. Then we apply the visual cryptographic decryption.

As we know that visual Cryptographic decryption does not need any type of decryption algorithm or computation. It uses human visual system for decryption which is the core advantage for which visual cryptography was developed. Now we can decrypt the original secret image by overlapping or stacking the shares.

Yet another way to create sub pixels would be to have only one third of the sub pixels colored dark. Therefore, when sub pixels of a larger white pixel are piled upon each other they would appear light gray and the piling of the sub pixels of a black pixel would result in dark gray. However, normal eye can comprehend the difference between gray and completely dark pixels better than two different fills of gray itself.

3. USAGE OF VISUAL CRYPTOGRAPHY

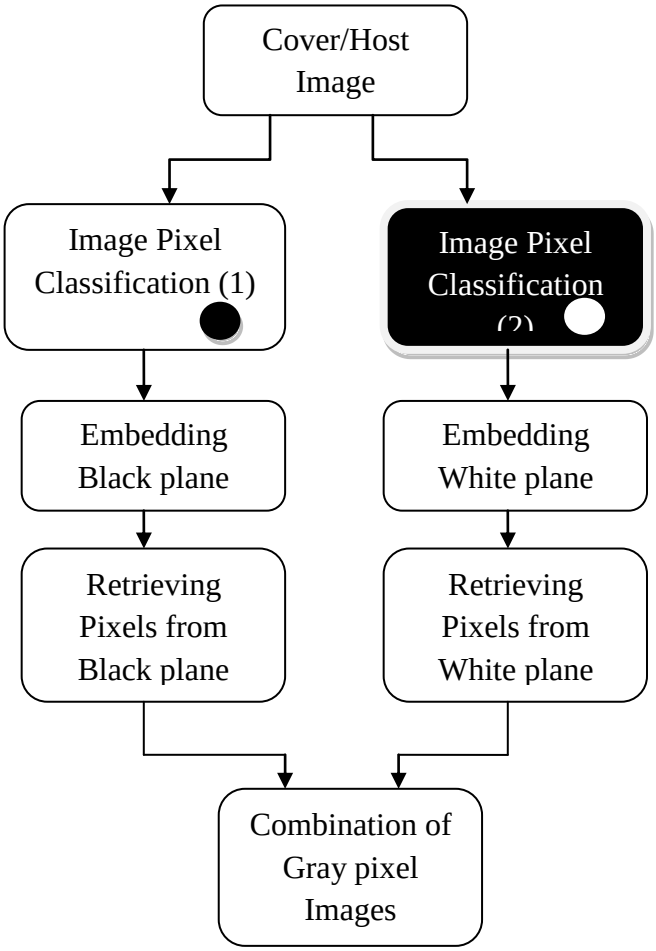

fig 2: Overall Flow diagram for n*n pixels

We observe that the distribution of subpixels also corresponds to the comparison based splitting of secrets in the case of text. However, in this case, each sub pixel can simply be represented by 1 bit. Their spatial distribution determines the manner in which they are piled and the color they produce in the retrieved image.

Assume the white queue is treated first. Each time, take n not-yet-treated white secret pixels from the white queue, and select a matrix from *C0* to express these n white sub-pixels. This *n*-by-n matrix is then divided into *n* columns: each white sub-pixel gets one column. For each column x, since it has *n* elements, each element y is passed to shadow y (for there are *n* shadows) to paint the pixel whose pixel coordinate (a, b) is exactly the picture element's location (a, b) of the white pixel x.

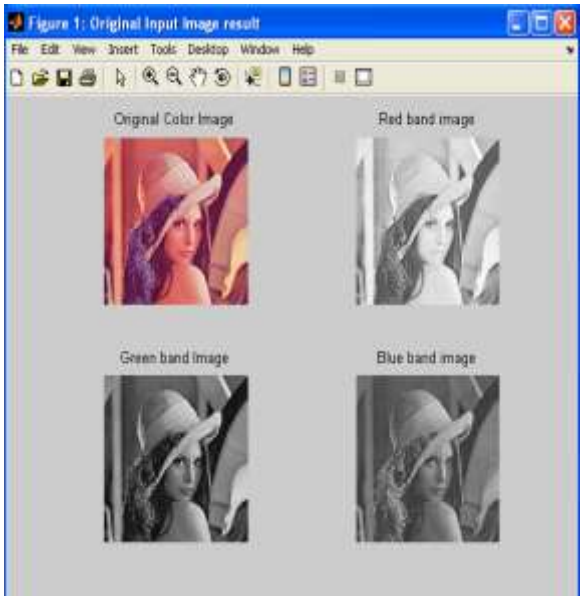

fig 3: Original input image & classified gray scale images – a subplot list

The optimality of VCS [16] is determined mostly by its pixel expansion n and the relative contrast. Pixel expansion m represents the passage in resolution from the original image to the decoded one. Therefore n needs to be as small as possible. In addition, m also needs to be in the form of *n*2 where *n 2 n* in order to preserve the aspect ratio of the original image.

On the other hand, the relative contrast needs to be as large as possible to ensure visibility. In the scope of this paper, we will only explore the tasks related to contrast optimization. Works related to retrieving lower bound of pixel expansion m can be found, etc. The research on contrast optimization was motivated by the problem of additional effects introduced to the derived image. This occurs because the decoded image is not an exact reproduction of the original image, but an expansion of the original, with extra black pixels.

The black pixels in the original image will remain black if d=n. However, the white pixels will become grey, due to the blackness introduced by the black sub-pixels, which resulted in loss of contrast to the entire image. It is not hard to show that a (n,n) threshold scheming.

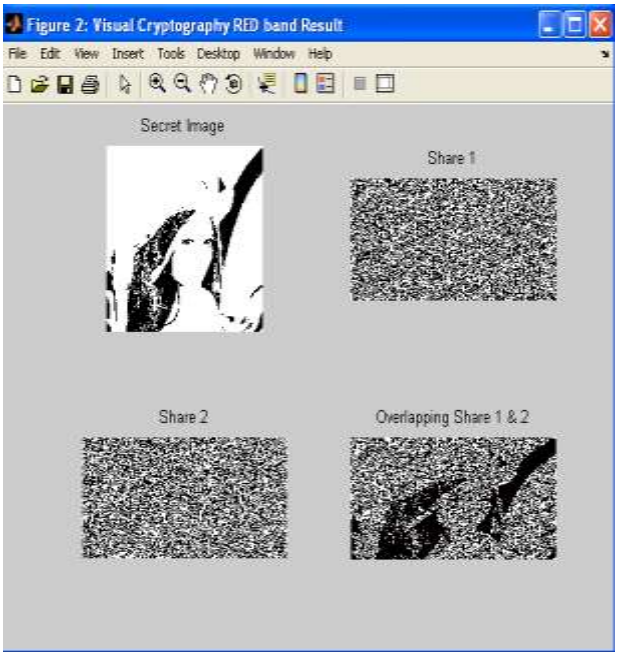

fig 4: VC (Visual Cryptography) for each sub band (RED band)

The VCS principle can also be applied in carrying confidential financial documents over Internet. VCRYPT [3] is an example of this type of system being proposed. VCRYPT can encode the original drawing document with a specified (y,n) VCS [10]. The decoding only requires bitwise "OR" operation on all shares in the specified directory, and needs no extra effort of cryptographic computation.

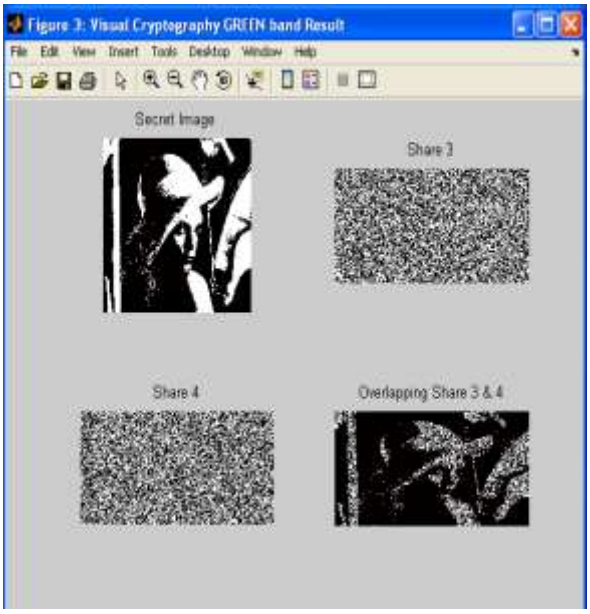

fig 5: Cryptography for Green Sub-band

Any malicious attacker who intercepts only m of n shares where n < *y* will not be able to gain any information about the financial document. Moreover, it is impossible to alter the content of the document unless all shares are intercepted, altered and re-inject into the network. Cryptography was an ultimate technique that uses the separation of frames, forming and collecting the sub-bands, based on pixels can also we can classify it.

This comes to a point that whatever the technique we include, our aim is to impart the technical aspects of data hiding. Financial documents often contain a lot of digits. Therefore, after applying VCS, we will expect that the graying effect will prevent us from recognizing the "fuzzy" digits in decoded documents.

4.RESULTS & DISCUSSIONS:

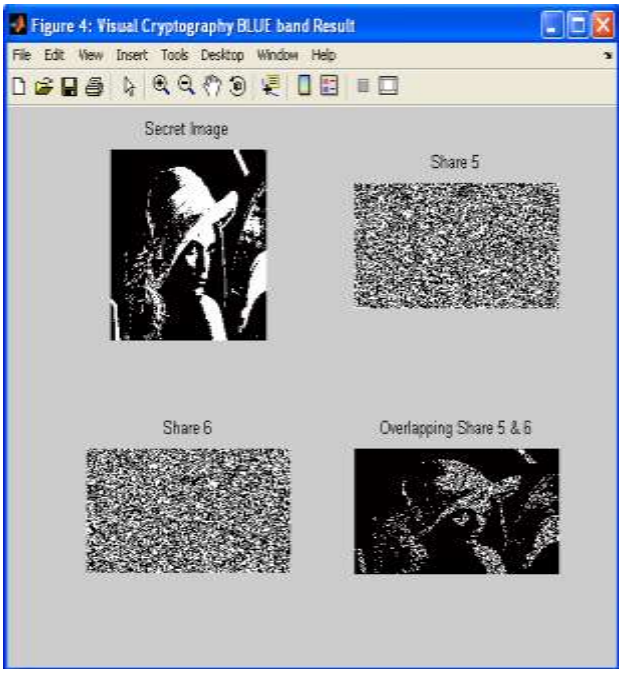

fig 6: Cryptography for Blue Sub-band

We can go for many types of secret data hiding or transferring ideas. Now-a-days, keeping the confidential data with high level of security is a quite challenging one. So, we can go for many emerging techniques of separating the data based on frame separation of blue lane, green plane and red plane.

And also, the recent trends in this tell us about the idea of separating the frame with the concern of Black sub-pixels, White sub-pixels, gray matters portioning, etc. Including the concept of various blue/green/red noise half toning into the construction theorem of conventional VC, the proposed method helps in visually pleasing the halftone contributions carrying the ultimate visual information.

The obtained visual tone is better than that attained by any other available VC method known to date. The new method can be broadly used in a number of visual secret sharing applications which require high-quality visual images, such as watermarking, electronic cash, etc. We have done with the technique of Cryptography with the new emerging trend of Visual Cryptography (VC). Such that, many data hiding techniques can also be implemented such as Steganography, stego data hiding, adaptive data embeds with pixel pairing method, etc. Above mentioned results tell us how to separate the frames into 3 various regions of sub-bands such as red, green and blue level of sub-bands.

REFERENCES

1. G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Extended capabilities for visual cryptography," *Theoret. Comput. Sci.*, vol. 250, no. 1–2, pp. 134–161, 2001.
2. R. A. Ulichney, "The void-and-cluster method for dither airay generation," in *Proc. SPIE, Human Vision, Visual Processing, Digital Displays IV*, Sep. 1996, vol. 1913, pp. 332–343.
3. M. Naor and A. Shamir, "Visual cryptography," *Adv. Cryptol.: EUROCRYPT, Lecture Notes Comput. Sci.*, vol. 950, pp. 1–12, 1995.
4. D. L. Lau and G. R. Arce, *Modern Digital Halftoning*. New York: Marcel-Dekker, 2000, pp. 52–89.
5. G. Di Crescenzo and C. Galdi, "Hypergraph decomposition and secret sharing," in *Proc. 14th Int. Symp. Algorithms and Computation, LNCS*, Sep. 1996, vol. 1913, pp. 332–343.
6. Horng, G., Chen, T. and Tsai D. 2006. Cheating in Visual Cryptography. *Design, Codes and Cryptography* 38:219-236.
7. C. Blundo, S. Cimato, and A. De Santis, "Visual cryptography schemes with optimal pixel expansion," *Theor. Comput. Sci.*, vol. 369, nos. 1–3, pp. 169–182, 2006.
8. C. Blundo, P. D'Arco, A. De Santis, and D. R. Stinson, "Contrast optimal threshold visual cryptography schemes," *SIAM J. Discrete Math.*, vol. 16, no. 2, pp. 224–261, 2003.
9. M. Bose and R. Mukerjee, "Optimal (*k*, *n*) visual cryptographic schemes for general *k*," *Designs Codes Cryptography*, vol. 55, no. 1, pp. 19–35, 2010.
10. Y.C. Hou, C.Y. Chang, and F. Lin, "VC for color images based on decomposition," *of 5th Conference on Information Management*, Taipei, Nov 1999, pp. 584–591.
11. Young-Chang Hou, "Visual cryptography for color images," *Pattern Recognition*, vol.36, pp.1619–1629, 2003.
12. B.S. Zhu, J.K.Wu, and M.S. Kankanhalli, "Print signatures for document authentication," in *Proc. of*

ACM Conference on Computer and Communications Security, October 2003, pp. 145–153.

13. N. Degara-Quintela and F. Perez-Gonzalez, "Visible encryption: using paper as a secure channel, security and watermarking of multimedia contents," in *Proc. Of SPIE'03*, 2003, vol. 5020.
14. G. Ateniese, C. Blundo, A. De Santis, and D. Stinson, "Extended schemes for visual cryptography," *Theoretical Computer Science*, vol. 250, pp. 143–161, 2001.
15. J. Weir and W. Yan, "A comprehensive study of visual cryptography," in *Transaction on Data Hiding and Multimedia Security V* (Lecture Notes in Computer Science, vol. 6010), Y. Q. Shi, Ed. Berlin/Heidelberg, Germany: Springer, 2010 pp. 70–105.
16. C.-N. Yang and T.-S. Chen, "Size-adjustable visual secret sharing schemes," *IEICE Trans. Fund am.*, vol. E88-A, no. 9, pp. 2471–2474, 2005.
17. S. J. Shyu, "Image encryption by random grids," *Pattern Recognit.*, vol. 40, no. 3, pp. 1014–1031, 2007.
18. S. J. Shyu, "Image encryption by multiple random grids," *Pattern Recognit.*, vol. 42, no. 7, pp. 1582–1596, Jul. 2009.
19. S. J. Shyu and M. C. Chen, "Optimum pixel expansions for threshold visual secret sharing schemes," *IEEE Trans. Information Forensics Security*, vol. 6, no. 3, pp. 960–969, Sep. 2011.

