A Secured Framework for Sharing Data using Diverse Image Media and Image Encryption

Ashish Singh
Department of Computer Engineering
SP'S IOK college of engineering Shirur, Savitribai Phule Pune University and Maharashtra India

Ajay Kumar Gupta
Department of Computer Engineering
SP'S IOK college of engineering Shirur, Savitribai Phule Pune University and Maharashtra India

Abstract

Secret images in shares that are either encoded and stored in a digital form or printed on transparencies or are hidden in Conventional visual secret sharing (VSS) scheme. Appearance of the shares as noisy-like pixels or as meaningful images; during the transmission of the shares it can cause suspicion and increase interception risk. Hence, transmission risk problem for the secret itself and for the involved participants in this scheme will be suffered in VSS schemes. To solve the transmission risk problem, we proposed a natural-image-based VSS scheme (NVSS scheme) in which secret images is shared via various carrier media so that the secret and the participants can be protected during the transmission. The proposed scheme can share one secret image over n selected natural images (called natural shares) and one noise-like share. Any kind of photos or hand-painted pictures in digital form or in printed form can be the natural shares. Based on these natural shares and the secret image the noise-like share is generated. The transmission risk problem can be reduced as the unchanged natural shares are diverse and innocuous. We also hide the noise like share to reduce the transmission risk problem. We have also used planned randomness in which during steganography the pixels are not stored in the carrier image original position instead the key is added to the original pixel position to obtain the new position which added additional security. Also we used alpha channel watermarking to find whether the images pixels are changed or not if changed then we can't get the original image.

Keywords: Visual secret sharing scheme, extended visual cryptography scheme, natural images, transmission risk

I. INTRODUCTION

The technique that encrypts a secret image into n shares, one or more shares holding by each participant is known as Visval cryptography (VC). No one can reveal the information about secret image if they hold less than n shares. The secret image can reveal and can be directly recognized by the human visual system by stacking the n shares. There are various types of secret images: photographs, handwritten documents, images, and others. Visual secret sharing (VSS) scheme is also the sharing and delivering secret images. To securely share the secret image is the original motivation of VC. As devices with computational powers are ubiquitous (e.g., smart phones) so in computer-aided environments, sharing visual secret images are today's important issue. In conventional shares, there are many random and meaningless pixels, and for protecting secret content it satisfy the security, but they suffer from two drawbacks: first, it holds noise-like shares which can cause attackers suspicion and increase interception risk so there is a high transmission risk. Because of the increase in the risk to both participants and the shares, the probability of transmission failure also increases. Second, because of the non-user friendly meaningless shares if there is increase in number of shares then the management of shares will become difficult and will never provide shares identification information.

To cope with the management issues, the Extended Visual Cryptography Scheme (EVCS) or the user-friendly VSS scheme in previous research provided some effective solutions. Shares are easily detected by the naked eye if it contains lot of noisy pixels or display images of low-quality and the shares transmitted by the participants can easily lead to suspicion by others. By using steganography techniques, secret images can be hidden into the cover images which are halftone gray images and true-color images. But by using steganalysis method, stego-images still can be detected. Thus the investigation of the existing VSS schemes must be done for reducing transmission risk problem for carriers and shares. In VSS schemes, a method for reducing transmission risk is an important issue. In this project, we proposed natural image based VSS scheme(NVSS scheme) to reduce the suspicion and intercepted risk in the transmission phase and also added more security to the secret image. Unity carrier (e.g., either digital or transparencies images) are used in Conventional VSS schemes for image sharing, which limits the VSS schemes practicality. In proposed project sharing of digital images by using diverse media. Hand-printed pictures, digital images, printed images and so on are contained in the carrier media. Degree of difficulty of intercepting the shares can be increased by applying diverse media for secret image sharing. The digital secret image can be shared over n-1 arbitrary natural images and one share in the proposed NVSS scheme. Each natural share features are extracted by the proposed approach instead of changing natural images contents. Thus the interception probability of these shares is greatly reduced as these unaltered natural shares are completely innocuous. To increase the security during transmission, the noise like generated share can be concealed using data hiding techniques. Diverse media is used as carrier in the NVSS scheme so it has many possible secret images sharing scenarios. For example, for sharing secret image assume a user selects n-1 media as natural shares. The dealer can choose an image that is not easily suspected as the content of the media (e.g., flysheets, landscape, hand-painted pictures, and portrait photographs,) to reduce the transmission risk. The digital

shares can be stored in a participant's digital devices (e.g., digital cameras or smart phones) to reduce the risk of being suspected. The printed media (e.g., flysheets or hand-painted pictures) can be sent via postal or direct mail marketing services. In such a way, the transmission channels are also diverse, further reducing the transmission risk. In a participant's digital devices (e.g., digital cameras or smart phones) the digital shares can be stored to reduce the suspicion risk. To reduce the transmission risk, the printed media (e.g., flysheets or hand-painted pictures) can be sent via diverse transmission channels i.e. through postal or direct mail marketing services. We have also used planned randomness in which during steganography the pixels are not stored in the carrier image original position instead the key is added to the original pixel position to obtain the new position which added additional security. Also we used alpha channel watermarking to find whether the images pixels are changed or not if changed then we can't get the original image. Proposed NVSS scheme has high level of manageability and user friendliness and also provide the high level security to the shares and participants and also reduces the transmission risk.

A. Problem Statement

We also propose excellent solution for solving the transmission risk problem. We have used planned randomness in which during encryption the pixels are not stored in the carrier image original position but instead the key is added to the original pixel position to obtain the new position which added additional security. We used alpha channel watermarking to check whether image pixels are changed or not.

B. Motivation

The motivation of my project is to increase the security level in image processing as it will be very useful in the image processing environment where high level security is important. And to provide high level of user friendliness and manageability, also to reduce the transmission risk and enhances security.

II. RELATED LITERATURE SURVEY

Existing researches only focused on using transparencies or digital media as carrier for VSS scheme. The transparency shares have either meaningful appearance or noise like which cause suspicion and increase intercepted risk. The conventional shares are not friendly [1]-[4]; so further researches are done to increase the friendliness of VSS schemes for participant [5][7]. The noise-like shares are added into the meaningful image for identification which makes traditional VC scheme friendly and easy to manage. But the display quality of the recovered image is reduced. With research in gray-level and color secret image results in the user friendly VSS scheme in which the cover images are added into the meaningless shares.[8]-[13]. Some study shows that the quality of shares are more than the recovered image display quality[8]-[11]. Then the display qualities of shares were enhanced in later researches. In other researches, stegnography techniques is used by the researchers which hides secret image into the cover image.[14]-[16]. This technique makes the communication invisible and reduces the suspicion risk.
Then the Chiu et al. researched on sharing secret image using natural images [18]. In this project we make the extension to the previous study for more security and reduce the transmission risk problem.

III. EXISTING SYSTEM

Previous research into user friendly VSS (visual cryptography scheme) provided some effective solutions to cope with the management issue. Also the shares appeared to be many noise-like pixels or display low-quality images easy to detect by the naked eye, lead to suspicion by others and increase interception risk. By using the stegnography techniques, secret images can be hidden into the cover images. However by using steganalysis methods, the stego-images still can be detected.

A. Disadvantages

- High transmission risk because holding noise like shares will cause attackers suspicion and the shares may be intercepted.
- We can't find that whether the meaningful share images are changed or not during transmission.

IV. PROPOSED SYSTEM

We proposed a natural-image-based VSS scheme (NVSS scheme) in which secret images is shared via various carrier media so that the secret and the participants can be protected during the transmission. The proposed scheme can share one secret image over n-selected natural images (called natural shares) and one noise-like share. Any kind of photos or hand-painted pictures in digital form or in printed form can be the natural shares. Based on these natural shares and the secret image the noise-like share is generated. We also hide the noise like share to reduce the transmission risk problem. We have also used planned randomness in which during steganography the pixels are not stored in the carrier image original position instead the key is added to the original pixel position to obtain the new position which added additional security. Also we used alpha channel watermarking to find whether the images pixels are changed or not if changed then we can't get the original image. And also we used alpha channel watermarking to find whether the pixels are changed or not.

A. System Architecture

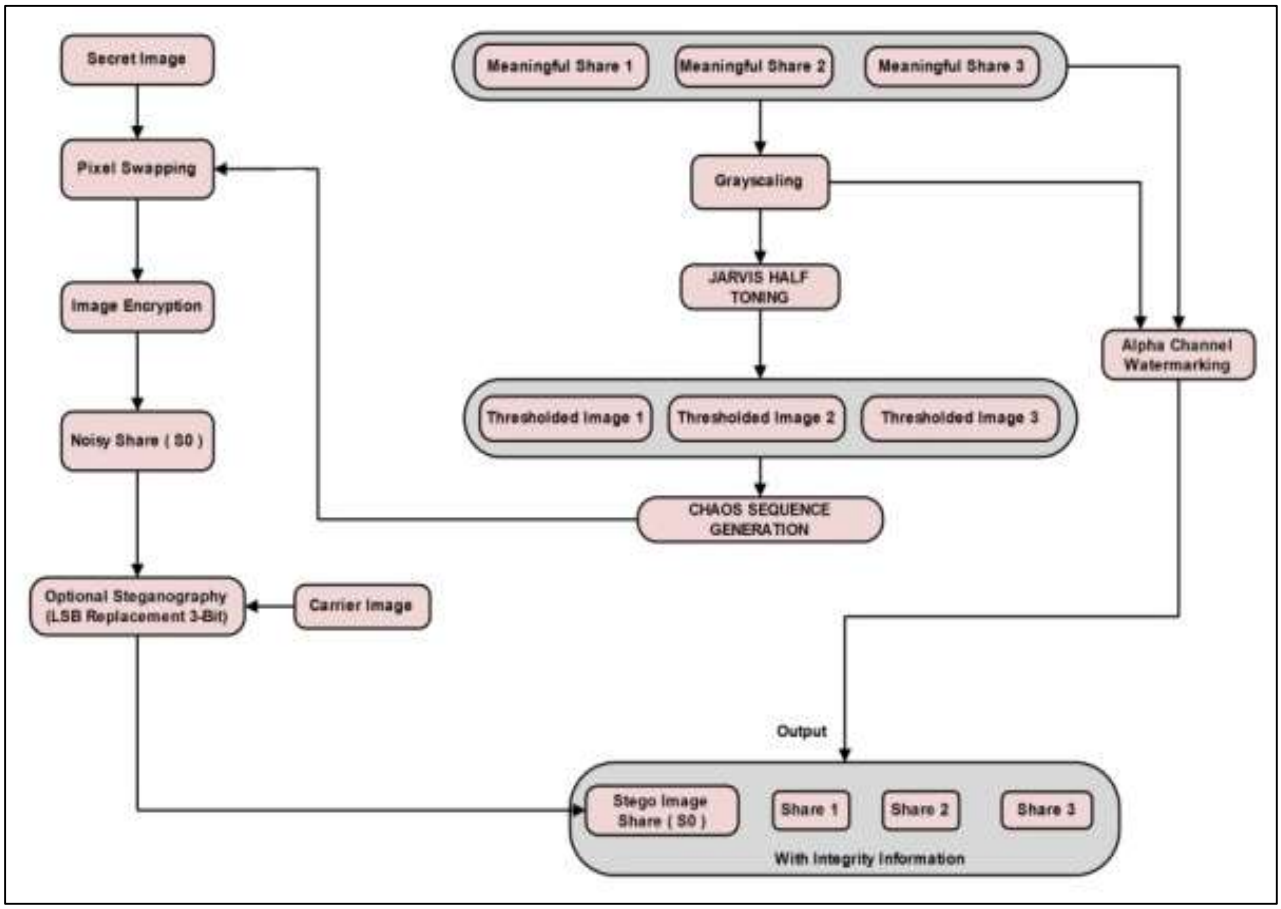

Fig. 1: Architecture

B. Overview of Algorithms

1) Jarvis Halftoning

Many image rendering technologies only have binary output. For example, printers have only two options i.e. "fire a dot" or not. Halftoning is a method for creating the illusion of continuous tone output with a binary device. Effective digital halftoning can substantially improve the quality of rendered images at minimal cost.

Thresholding: It is the simplest method of image segmentation. Thresholding can be used to create binary images from the grayscale image

In the normal thresholding we need to manually select the threshold value but in Jarvis halftoning, the threshold value is decided by the nearby pixel value.

2) Henon map encryption

During the pixel swapping, the pixels are swapped in the certain way so that the attacker will not get the order of original pixels position. This order is explained by this:

Consider x0 and y0 be the position of pixels. X1 and Y1 be the new position of pixels after swapping. Then the new pixel positions will be:

$$X1= 1+y0(\alpha*x0)$$
$$Y1=(\beta*x0)$$

Where $\alpha = 0.3$ and $\beta = 0.7$

3) LSB Replacement

In steganography the digital media mainly digital images are used as a medium for hiding information and the information in the form text, digital image, video or audio file may be used as secret message. The word steganography derived from two Greek words: steganos means covered and graphos means writing and often refers to secret writing or data hiding. In the LSB replacement the secret image bits are hidden into the LSB last 3 bits of all R, G and B pixel.

4) Alpha Channel Watermarking

These watermarking is used to check whether the images pixels are changed or not because if the pixels of the shared images are changed then we cannot get the secret image as the key will not be generated. So alpha channel watermarking is used to verify the

pixels. We normally use 24 bits to store value of pixels but here we use 32 bits. Where starting 8 bit the alpha value is stored. The alpha value will be the sum of R, G and B divided by 3.

$$\alpha = (R+G+B)/3$$ where α is the alpha value before transmission.

And after transmission we need to find Qs which is the new alpha value.

$$Qs = (R+G+B)/3$$

If α==Qs then the pixels are unchanged hence we can get the secret image.

C. *Advantages*

- High security
- User friendly
- Key not generated until we get the 3 images.

D. *Flow Chart:*

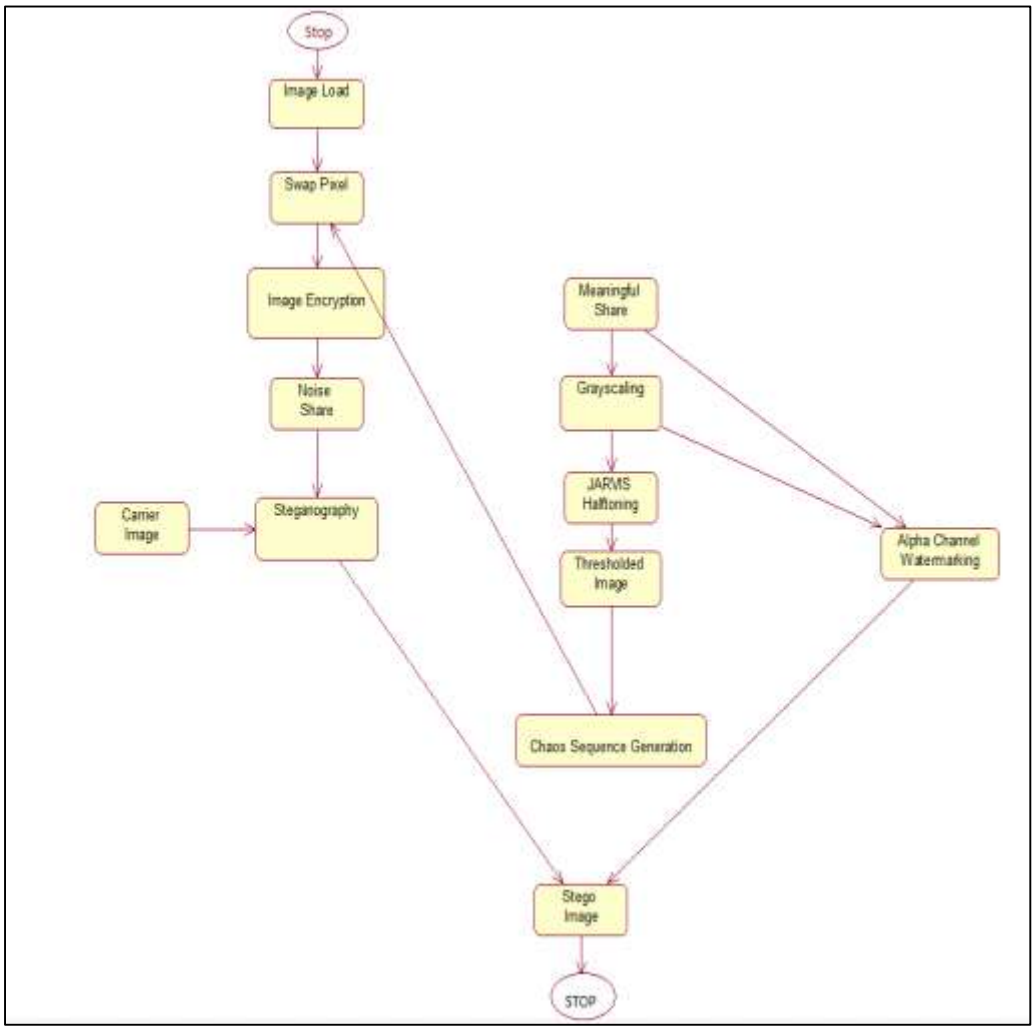

Fig 2: Flow Chart

V. MATHEMATICAL MODELS

The mathematical model is a description of a system using mathematical concepts and languages. For system explanation and study the different components effects, mathematical is used.

A. *Set Theory:*

Let G be the global set
G = {U,IP,OP,K,A}
U -> Sets of users.
U = {u_1,u_2,u_3,u_4….un} Where n =∞.

IP -> Sets of input images.
IP = $\{I_{P1}, I_{P2}, I_{P3}, \ldots, I_{pk}\}$ Where $k \neq \infty$.
OP -> Sets of output images.
IP = $\{O_{P1}, O_{P2}, O_{P3}, \ldots, O_{Pk}\}$ Where $k \neq \infty$.
K -> Set of Encryption Keys.
K = $\{K_1, K_2, \ldots, K_n\}$ Where $n = \infty$.
A -> Set of all Algorithms.
A = $\{A_1, A_2, A_3, \ldots, A_k\}$ Where $k \neq \infty$.

B. MORPHISM:

B_{i1},B_{i2},B_{i3} <- Load meaningful shares(S_1,S_2,S_3);
G_{s1},G_{s2},G_{s3} <- Apply Grayscale(B_{i1},B_{i2},B_{i3});
T_{h1},T_{h2},T_h <- Apply Jarvishalftoning(G_{s1},G_{s2},G_{s3});
<key> <- generate EncryptionKey(T_{h1},T_{h2},T_{h3});
S_{Bi} <- Load Secret images(Sec1);
E_{Bi} <- Apply Henon Map Encryption(SBi, <key>,α, β) (noisy share)
Stego $_{Bi}$ <- Apply stegnography(E_{Bi}, key);
Wm1, Wm2, Wm3 <- Apply watermarking (B_{i1},B_{i2},B_{i3});

C. Feasibility Tests:

In our project all the algorithm we have used are p-complete algorithm except Jarvis halftoning and Henon Map Encryption algorithm.

VI. RESULT OF PRACTICAL WORK

Fig. 3: Select Option Encryption

Fig. 4: Grayscale image

Fig. 5: Threshold Image

Fig. 6: Upload Secret Image.

Fig. 7: Apply Stegonography.

A. Now Decryption

Fig. 8: Apply Destegonography.

Fig. 9: Load 3 images to obtain the secret image.

Fig. 10: Decryption of secret image to get FINAL IMAGE

B. For Watermark Verification

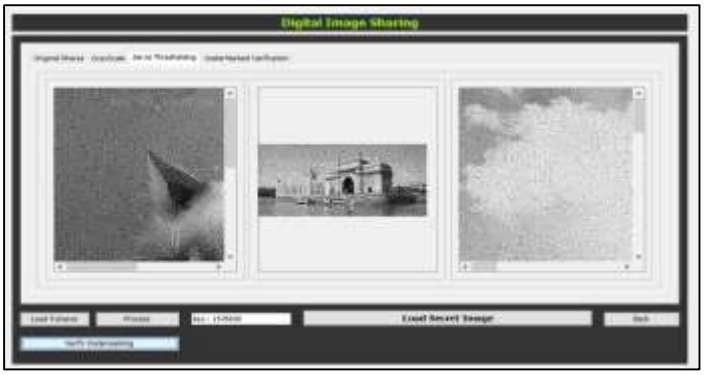

Fig 11: select option Verify watermaking

Fig. 12: Select 3 .tga images and check whether images are unchanged or not.

VII. CONCLUSION

Our project can share a digital image using diverse image media. The proposed project can provide high level security and effectively reduce transmission risk and provide the highest level of security.

VIII. FUTURE SCOPE

The future scope of our project is that we can use more other high accuracy algorithm instead of Henon map algorithm for pixel swapping. Also we can use more meaningful shares instead of 3 which we have taken in our project.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," in Advances in Cryptology, vol. 950. New York, NY,USA: Springer-Verlag, 1995.
[2] R. Z.Wang, Y. C. Lan, Y. K. Lee, S. Y. Huang, S. J. Shyu, and T. L. Chia, "Incrementing visual cryptography using random grids," Opt. Commun.,vol. 283, no. 21, pp. 4242–4249, Nov. 2010.
[3] P. L. Chiu and K. H. Lee, "A simulated annealing algorithm for general threshold visual cryptography schemes," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 992–1001, Sep. 2011.
[4] K. H. Lee and P. L. Chiu, "Image size invariant visual cryptography for general access structures subject to display quality constraints," IEEE Trans. Image Process., vol. 22, no. 10, pp. 3830–3841, Oct. 2013.
[5] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, "Extended capabilities for visual cryptography," Theoretical Comput. Sci., vol. 250, nos. 1–2, pp. 143–161, Jan. 2001.
[6] C. N. Yang and T. S. Chen, "Extended visual secret sharing schemes: Improving the shadow image quality," Int. J. Pattern Recognit. Artif. Intell., vol. 21, no. 5, pp. 879–898, Aug. 2007.
[7] K. H. Lee and P. L. Chiu, "An extended visual cryptography algorithm for general access structures," IEEE Trans. Inf. Forensics Security, vol. 7, no. 1, pp. 219–229, Feb. 2012.
[8] Z. Zhou, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography," IEEE Trans. Image Process., vol. 15, no. 8, pp. 2441–2453, Aug. 2006.
[9] Z. Wang, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography via error diffusion," IEEE Trans. Inf. Forensics Security, vol. 4, no. 3, pp. 383–396, Sep. 2009.
[10] I. Kang, G. R. Arce, and H. K. Lee, "Color extended visual cryptography using error diffusion," IEEE Trans. Image Process., vol. 20, no. 1, pp. 132–145, Jan. 2011.
[11] F. Liu and C. Wu, "Embedded extended visual cryptography schemes," IEEE Trans. Inf. Forensics Security, vol. 6, no. 2, pp. 307–322, Jun. 2011.
[12] T. H. Chen and K. H. Tsao, "User-friendly random-grid-based visual secret sharing," IEEE Trans. Circuits Syst. Video Technol., vol. 21, no. 11, pp. 1693–1703, Nov. 2011.
[13] T. H. N. Le, C. C. Lin, C. C. Chang, and H. B. Le, "A high quality and small shadow size visual secret sharing scheme based on hybrid strategy for grayscale images," Digit. Signal Process., vol. 21, no. 6, pp. 734–745, Dec. 2011.
[14] D. S. Tsai, G. Horng, T. H. Chen, and Y. T. Huang, "A novel secret image sharing scheme for true-color images with size constraint," Inf. Sci., vol. 179, no. 19, pp. 3247–3254, Sep. 2009.
[15] X. Wu, D. Ou, Q. Liang, and W. Sun, "A user-friendly secret image sharing scheme with reversible steganography based on cellular automata," J. Syst. Softw., vol. 85, no. 8, pp. 1852–1863, Aug. 2012.
[16] C. Guo, C. C. Chang, and C. Qin, "A multi-threshold secret image sharing scheme based on MSP," Pattern Recognit. Lett., vol. 33, no. 12, pp. 1594–1600, Sep. 2012.
[17] A. Nissar and A. H. Mir, "Classification of steganalysis techniques: A study," Digit. Signal Process., vol. 20, no. 6, pp. 1758–1770, Dec. 2010.
[18] P. L. Chiu, K. H. Lee, K. W. Peng, and S. Y. Cheng, "A new color image sharing scheme with natural shadows," in Proc. 10th WCICA, Beijing, China, Jul. 2012, pp. 4568–4573.
[19] Qin Chen, Wen-Fang Pengo Min Zhang, Yi-Ping Chu," An (n, n) threshold Visual Cryptography Scheme for Cheating prevention", 978-1-4244-5540-9/10/$26.00 ©2010 IEEE