International Journal of Electronics Engineering (ISSN: 0973-7383
Volume 11 • Issue 1 pp. 322-328 Jan 2019-June 2019 www.csjournals.com

Secret Gray Scale Image Sharing using Meaningful and self Authenticating Shares

Abhishek dwivedi[1], Arun Kumar Shukla[2]
[1]Student, [2]Assistant Professor
Department of Computer Science and Information Technology, Vaugh Institute of Agriculture, Engineering and Technology, Sam Higginbottom University of Agriculture, Technology and Sciences, Prayagraj, India

Abstract: This paper proposes a Secret Gray Scale Image Sharing using Meaningful and self Authenticating Shares. This scheme overcomes various problems of existing secret sharing schemes such as problem of pixel expansion, random shares and share authentication. Using proposed approach one can secretly share a gray scale image into two meaningful gray scale shares. Both the shares will have tamper detection property by which they can authenticate themselves for any alteration or attacks. Both the shares are unexpanded and meaningful in nature which reduced the vulnerability for cryptanalysis and save the bandwidth for transmission . Experimental results show that if there is no attack on any of the shares then the imperceptibility between the recovered secret and the original secret will always be infinite and the proposed approach has good tamper detection capabilities up to 95 % also it takes less time in order to encode and decode the secret image.
Key words: Secret sharing, Self authentication, Meaningful shares. Unexpanded shares, Share authentication.

I Introduction

Secret sharing is very vital application of Visual Cryptography (VC). Secret may be image, speech or video. In this paper gray scale image has been taken in our consideration. When an image is transmitted via internet then it is very necessary to encode the image so that only an authority with valid decryption secret key can only take enjoy of that secret image. In this paper fundamental of visual cryptography is used to encode an image.

Visual cryptography (VC) is a technique for secret sharing, which is first proposed by Naor et al. [11]. VC permits the decryption of concealed images without the help of any computation. In a k-out-of-n visual secret sharing (VSS) scheme, an image is encoded into the form of n number of random shares. Random share means each share looks like an unsystematic binary pattern. Finally the shares are then printed onto transparencies. These transparencies will be treated like a secret key and will distributed among n participants. Since isolated share has no information related to secret image but one can see the secret visually by just stacking any k or more transparencies of the shares without any calculation. Infinite computation power can also not be able to decode the secret with, $k - 1$ or fewer participants. There are many other applications like access control, copyright protection [12], watermarking, identification [13] and visual authentication where visual cryptography could be used. One can understand the method of VSS by following example:

Consider a trivial 2-outof- 2 Visual secret sharing ($k = 2; n = 2$) scheme shown in Figure. 1. Each pixel p of secret binary image is encoded into a pair of black and white subpixels for both shares. If p is white/black, one of the first/last two columns tabulated under the white/black pixel in Fig. 1 is selected randomly so that selection probability will be 50%. Then, the first two subpixels in that column are alloted to share 1 and the following other two subpixels are alloted to share 2. Irrespective of the color of the pixel whether black or white, it is encoded into two subpixels of black-white or white-black with equal probabilities. Thus

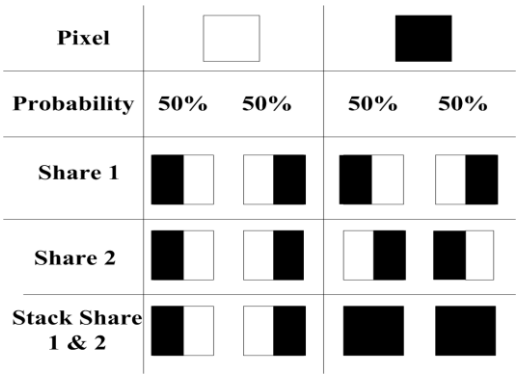

Fig. 1. Codebook for 2-out of 2 VSS scheme.

single share can not decide whether the given pixel p is black or white . stacking of both the shares are shown in the last row of Fig. 1. Black pixel p in input secret image leads two black subpixels as an output which corresponds to a grey level 1. Whereas white pixel p in input secret image leads one black and one white subpixels as an output which corresponds to a grey level 1/2. Thus by this way one can obtain the complete pseudo visual information without recovering the all pixels.

One can see the drawbacks of the existing secret sharing approach that are:

1. One cannot share non binary images by this rule.
2. One cannot be able to recover the complete secret image with full accuracy
3. Shares are expended in their size which is major drawback.

So, In this paper we have considered all these issue in our account and developed a novel approach which will be able to secretly share a gray scale image with meaningful shares without pixel expansion.

Due to latest advancements in the multimedia technology, image may be very easily altered. Verifying the integrity of the image is a very vital issue in many areas like court evidences There are various good multimedia alteration tools available nowadays by which tampering of the images are very easy task. Hence declaration for the authenticity of multimedia content is an important topic of concern for current era [3]. Image hashing is one of the technique which is the result of prevention approach for this type of alteration . Fragile watermarking is also a very good approach to ensure the integrity of the any given multimedia content. Watermarking not only allows to check the integrity of the given image , but also it is used to provide the ownership assertion of the given images. Image hashing maps an input image to a short string, called image hash, and has been widely used in image retrieval [1], image authentication [4], digital watermarking [5], image copy detection [6], tamper detection [7], image indexing [8], multimedia forensics [9], and reduced-reference image quality assessment [10]. In the proposed approach, we have used self authentication method in order to protect the integrity of the shares. Ateniese et al. [14] proposed the method of extended visual cryptography (EVC). In EVC, the shares contain both, shares are meaningful in nature but secret images can still be exposed only when qualified shares are stacked together. Shares of EVC scheme, however, provide very low visual quality as they are restricted only for binary images. Nakajima et al. [15] improved the current form of EVC approach for gray scale images in order to provide more visually appealing images. Shyong jian [16] proposed a visual cryptography approach for color images but he suffered with problem of share randomness. To make meaningful shares, A Halftone Visual Cryptography (HVC) is proposed by Zhou and Arce [18], which is more improved version of EVC. The main drawback of HVC approach is the pixel expansion. Zhonmin et al. [17] has proposed more extended version of HVC in which complimentary shares is replaced by the Auxiliary Black Pixel(ABP). Another time the shortcoming of this approach is pixel expansion.

II Proposed Approach

Propose approach is divided into four major steps as shown in figure 2. First two steps are handled at the sender side whereas last two steps are handled at receiver side. In first approach we generate meaningful shares for a secret image. In second step generated shares are upgraded with self authenticating property. We check for any alteration on share in step 3. If both shares are authentic then we can successfully perform recovery operation as mentioned in step 4.

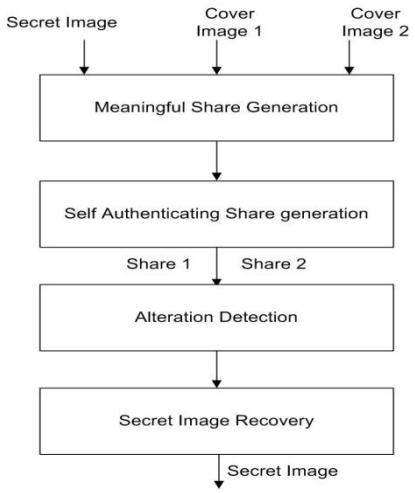

Figure 2- Flow Diagram of Proposed approach

International Journal of Electronics Engineering (ISSN: 0973-7383
Volume 11 • Issue 1 pp. 322-328 Jan 2019-June 2019 www.csjournals.com

2.1 Meaningful share generation

In this step, we generate two meaningful shares to secretly share a single gray scale secret image. Both shares will also be gray scale in nature. Meaningful shares mean both will have some visual meaningful information rather than randomness. In order to create meaningful shares we consider following steps:

Step 1- Take an Input gray scale image I of size $M \times N$ and two cover images C_1 and C_2 of same size $M \times N$ which will be displayed on the shares, where M and N both are divisible by 4.

Step 2- Resize the Image I by $\frac{M}{2} \times \frac{N}{2}$.

Step 3- Divide the cover image C_1 and C_2 into non overlapping blocks of size 2×2.

Step 4- Covert the input image I into one dimensional vector form V. Now each pixel of the vector V corresponds to each block of C_1 and C_2.

Step 5- Covert the pixel intensities of vector V, C_1 and C_2 in eight bit binary format.

Step 6- Now take the four LSBs of i^{th} intensity of vector V and embed them into first LSBs of the four pixels of i^{th} block of C_1. Similarly, take the four MSBs of i^{th} intensity of vector V and embed them into first LSBs of the four pixels of i^{th} block of C_2.

Step 7- Convert all binary value s of the pixels into decimal format.

Step 8 – Now this embedded cover images will be called meaningful shares S_1 and S_2. Here the cover information will dominate on the secret image information hence one can only see the information of the cover image.

2.2 Self Authenticating Share generation

Once we get the meaningful shares, we need to upgrade it by another property i.e. self authenticity. As we know that shares are very sensible objects carrying the vital information of the secret image. Hence it may be tampered intentionally or unintentionally in between the transmission. Hence all shares must be capable enough to detect its alteration region without the help of original one. This type of alteration detection is called blind alteration detection. To create self authentication shares we perform following operation:

Step 1- Take the meaningful Shares S_1 and S_2 as input.

Step 2- Generate two Random vectors R_{v1} and R_{v2} of size $1 \times M$ and $1 \times N$ respectively using two different symmetric keys k_1 and k_2 .

Step 3- Pick pixel P_1 of $S_1(i,j)$ and pick a pixel P_2 of index $S_1(R_{v1}(i), R_{v2}(j))$, where i and j range from 1 to M and 1 to N respectively.

Step 4- Perform bit wise ExOr operation between P_1 and P_2 (for six bits excluding first two LSBs)and get resultant pixel P.

Step 5- Now apply following bitwise operation on P:

$$b1 = \sum_{k=1}^{6} P_k \bmod 2$$

Step 6 – Embed the bit b_1 into the second LSB of pixel $S_1(i,j)$.

Step 7 – Apply the same operation for all the pixels of S_1 and the resultant image is called self authenticating share.

Step 8- Repeat the Step 2 to Step 7 for meaningful share S_2 usig two different symmetric keys k_3 and k_4.

International Journal of Electronics Engineering (ISSN: 0973-7383
Volume 11 • Issue 1 pp. 322-328 Jan 2019-June 2019 www.csjournals.com

2.3 Alteration Detection

This step is performed at receiver side. Once receiver receives the shares he will ensure that he has got the authenticated shares. To ensure it, he will detect the alteration for both the shares using following approach. If receiver finds any alteration then he will ask another fresh share from the sender side.

Step 1- Extract the second LSB from each pixel of share S_1 as well as S_2 and make a binary matrix M_1 of size $\times N$.

Step 2- Recalculate b_1 for all the pixels of S_1 and S_2 using same process by which they were generated.

Step 3- Create a binary matrix M_2 for both the matrices using b_1.

Step 4- Do pixel wise comparison between M_1 and M_2. If both pixels are same then mark it as black i.e. unaltered else white i.e. altered.

2.4 Secret Image Recovery

If receiver detects no alteration in any of the shares then he can recover the secret using following steps. We can verify the quality of the recovered secret image by various methods which we will see in next section.

Step 1- Take meaningful self authenticating shares S_1 and S_2 as input.

Step 2- Divide both the shares into non overlapping blocks of size 2×2.

Step 3- Take first LSBs from each pixel of i^{th} block of size 2×2 of S_1 and take first LSBs from each pixel of i^{th} block 2×2 of S_2.

Step4- Append both the set of bits (four LSBs of S_1 and four LSBs of S_2).

Step 5- Convert the eight bit binary into the decimal format which will indicate the i^{th} pixel intensity of the secret image I.

Step 6- Repeat the same process for each block of the S_1 and S_2 both and the create an image by calculated pixels that will be the recovered image

III Experimental Result and Analysis

Proposed approach has been implemented in MATLAB 2015, window 7 (operating system)with processor intel core 2 duo . Experimental results show two meaningful shares for a gray scale secret image and again its upgraded version for self authentication. We have also performed many attacks on the shares and detected the alterations which are shown in the experimental results.

Figure 3- Example of Meaningful and Self authenticating Shares and Recovery of secret without any attack.

Figure 3 demonstrate the results of meaningful and self authenticating share generation. Image (a) shows the gray scale secret image which are going to be secretly shared. Image (b) and (c) shows the meaningful shares with dominating cover information. We can see that both the shares are also in gray scale in nature. Now image (d) and (e) show the results after embedding the self authenticating bits into the meaningful shares. We can see that there are no much difference in visual appearance of the images. We will see the same quantitatively. Figure (f) shows the recovered image from the shares. As in this example there are no attacks performed on the shares, hence we get the complete image without any distortion.

Figure 4- Example of tamper on the share, alteration detection and recovery with the altered shares.

Figure 4 demonstrates the efficiency of the proposed approach for the alteration detection. Here we can see that figure (a) is treated as secret image and secretly shared with two meaningful and self authenticating shares shown in (b) and (c). Let us consider that an attacker has done some intentional attack (written some objectionable text on the shares) on share 2. Now at the receiver side, there is no information related to the original shares. Receiver has only tampered share. This is a challenge for the receiver that only with the help of tampered shares, he has to confirm that the shares are not authentic. Receiver will apply our algorithms in order detect the alteration. Figure (f) and (g) are the results of tamper detection. Here black pixels show the unaltered region whereas white pixels show the altered one. As share 2 is altered hence we can see the tamper detection in the corresponding figure (g). Here we can see that we are not getting complete white pixels for the tamper detection this scenario is called false rejection. Finally figure (h) shows the result of the recovery using tampered shares. Figure (h) is not exactly same as the original image. Once the receiver will identify that a particular share is unauthentic then he will ask to the sender to send the corresponding share. Table 1 demonstrates the quantitative analysis for the tamper detection capabilities for the proposed approach. Here we can see that we are achieving very good accuracy for the alteration detection. If we see with respect to time then we will realize that the proposed approach is time efficient also.

Table 1- Tamper detection results for multiple secret images.

Secret Image	Altered pixel in Share 1	Altered pixel in Share 2	Detected Pixels in Share 1	Detected Pixels in Share 2	Accuracy %	Time in Second
Lena	340	95	310	81	88	50
Barbara	526	587	498	473	92	72
Boat	120	631	102	601	90	56
Cameraman	423	864	401	834	95	63
Girl	342	542	322	501	93	77

Figure 5 demonstrate the plot between number of altered pixel and detected pixels. Straight line shows the effectiveness of the proposed approach.

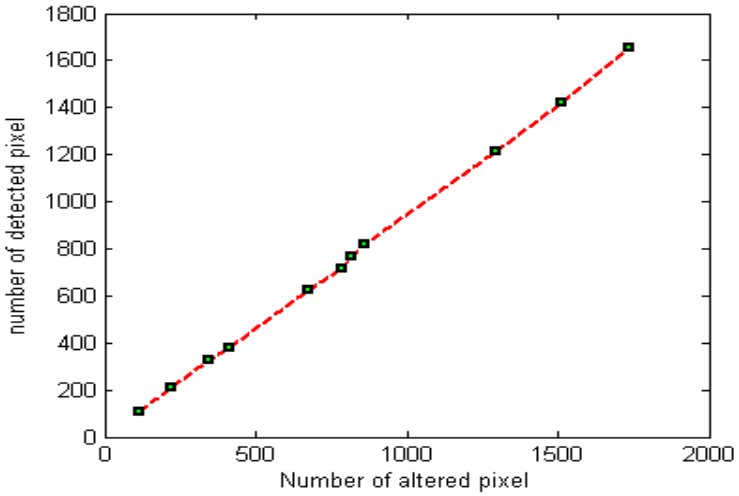

Figure 5: Plot between altered and detected pixels.

Proposed approach is unique from one more perspective. If there is no attack on any of the meaningful and self authenticating shares then the imperceptibility between the recovered secret and the original secret will always be infinite which is a great achievement of the proposed approach.

IV Conclusion

This paper proposes Secret Gray Scale Image Sharing using Meaningful and self Authenticating Shares by which one can secretly share a gray scale image into two meaningful gray scale shares. Both the shares will have self authenticating property by which they can authenticate themselves for any alteration or attacks. Both the shares are unexpanded in nature by which they distinguish themselves from other existing approaches.
If there is no attack on any of the shares then the imperceptibility between the recovered secret and the original secret will always be infinite which is a great achievement of the proposed approach. Experimental results show that the proposed approach has good tamper detection capabilities up to 95 % also it takes less time inorder to encode and decode the secret image.

References

[1] M. Slaney and M. Casey, “Locality-Sensitive Hashing for Finding Nearest Neighbors,” IEEE Signal Processing Magazine, vol. 25, no. 2, pp.128-131, Mar. 2008.
[2] M.N. Wu, C.C. Lin, and C.C. Chang, “Novel Image Copy Detection with Rotating Tolerance,” J. Systems and Software, vol. 80, no. 7, pp. 1057-1069, 2007.
[3] S. Wang and X. Zhang, “Recent Development of Perceptual Image Hashing,” J. Shanghai Univ. (English ed.), vol. 11, no. 4, pp. 323-331, 2007.
[4] F. Ahmed, M.Y. Siyal, and V.U. Abbas, “A Secure and Robust Hash-Based Scheme for Image Authentication,” Signal Processing, vol. 90, no. 5, pp. 1456-1470, 2010.
[5] C. Qin, C.C. Chang, and P.Y. Chen, “Self-Embedding Fragile Watermarking with Restoration Capability Based on Adaptive Bit Allocation Mechanism,” Signal Processing, vol. 92, no. 4, pp. 1137- 1150, 2012.
[6] C.S. Lu, C.Y. Hsu, S.W. Sun, and P.C. Chang, “Robust Mesh-Based Hashing for Copy Detection and Tracing of Images,” Proc. IEEE Int’l Conf. Multimedia and Expo, vol. 1, pp. 731-734, 2004.
[7] Z. Tang, S. Wang, X. Zhang, W. Wei, and S. Su, “Robust Image Hashing for Tamper Detection Using Non-Negative Matrix Factorization,” J. Ubiquitous Convergence and Technology, vol. 2, no. 1, pp. 18-26, 2008.
[8] E. Hassan, S. Chaudhury, and M. Gopal, “Feature Combination in Kernel Space for Distance Based Image Hashing,” IEEE Trans. Multimedia, vol. 14, no. 4, pp. 1179-1195, Aug. 2012.
[9] W. Lu and M. Wu, “Multimedia Forensic Hash Based on Visual Words,” Proc. IEEE Int’l Conf. Image Processing, pp. 989-992, 2010.
[10] X. Lv and Z.J. Wang, “Reduced-Reference Image Quality Assessment Based on Perceptual Image Hashing,” Proc. IEEE Int’l Conf. Image Processing, pp. 4361-4364, 2009.
[11] M. Naor and A. Shamir, “Visual cryptography,” Advances in Cryptograhy: EUROCRYPT94, LNCS, vol. 950, pp. 112, 1995.
[12] M. S. Fu and O. C. Au, “Joint visual cryptography and watermarking,” in Proc. IEEE Int. Conf. Multimedia and Expo, Taipei, Taiwan, Jun. 2004.
[13] M. Naor and B. Pinkas, “Visual authentication and identification,” Crypto97, LNCS, vol. 1294, pp. 322340, 1997.
[14]Ateniese G, Blundo C, De Santis A, Stinson DR (2001) Extended capabilities for visual cryptography. Theor Comput Sci 250:143–161
[15] Nakajima M, Yamaguchi Y (2002) Extended visual cryptography for natural images. In: J. WSCG, vol 10, pp 303–310

[16] Shyu SJ (2007) Image encryption by random grids. Patt Recog 40(3):1014–1031
[17] Wang Z, Arce GR, Crescenzo GD (2009) Halftone visual cryptography via error diffusion. IEEE Trans Inf Forensics Secur 4(3):383–396
[18]Zhou Z, Arce GR, Di Crescenzo G (2006) Halftone visual cryptography. IEEE Trans Image Process 15(8):2441–2453