Webology (ISSN: 1735-188X)
Volume 18, Number 6, 2021

A Modified 2-By-2 Vcs Scheme For Transmission Of Fingerprints Treated As 2d Textual Data: An Analytical Approach

Abhishek Garg[1] and Kishan Pal Singh[2]

[1]Department of Computer Engineering & Applications, Mangalayatan University, Aligarh, UP

[2]Department of Mechanical Engineering, Mangalayatan University, Aligarh, UP

CorrespondingAuthorsEmail:[1]abhishek47722@gmail.com,[2]kishan.singh@mangalayatan.edu.in

ABSTRACT:

Visual Cryptography is secret sharing of images to a group of participants. The existing 2-by-2 visual cryptography suffers from pixel expansion and poor image quality. A modified approach is suggested just not to only simplify this existing scheme but making it suitable to work for black & white images, creating shares & stacking them using XNOR operation. The hidden image behind the shares is restored with no pixel expansion and doing so with least distortion. Steganography is used to digitally watermark the images behind the shares adding security to the current scheme.

KEYWORDS:

Cryptography, Stegnography, Watermarking, Visual Cryptography.

INTRODUCTION:

Securing shares using 2-by-2 VCS is an efficient approach thereby using Visual cryptography based scheme that distinguishes machine and human. No complex mathematical operations are needed in this scheme as required in other RSA based cryptography techniques.

Following diagram in Fig.1 shows 2-By-2 VCS scheme with 2 sub pixel layout. The original image is hidden with 2 binary shares using VCS & these shares are superimposed to get back the original image.

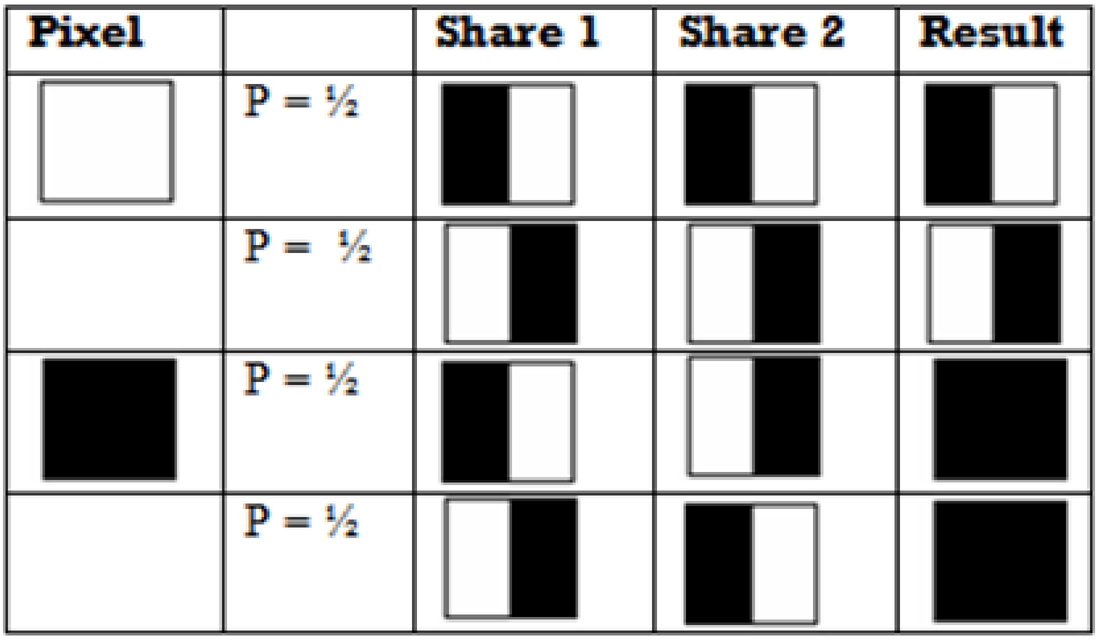


Fig.1. 2-By-2 VCS Visual Cryptography Scheme

Above scheme uses XNOR operation instead of other popular operations used by previous algorithms. Less pixel expansion using 2 sub pixel layouts with better contrast makes this algorithm more effective. The shares of black & white pixel is coded with 2 sub pixels each, having half percentage of black and white contrast in each share using different pattern in each Original black & white pixel encoding C_0 & C_1 as shown in Fig.2. But stacking these shares generates white pixel with less contrast but black pixel with more contrast.

$$C_0 = \left\{ \begin{bmatrix} 01 \\ 01 \end{bmatrix} \begin{bmatrix} 10 \\ 10 \end{bmatrix} \right\} \qquad C_1 = \left\{ \begin{bmatrix} 01 \\ 10 \end{bmatrix} \begin{bmatrix} 10 \\ 01 \end{bmatrix} \right\}$$

Fig 2. Black & white pixel pattern

RELATED WORK:

Original work is done by encryption of the given digitized data using simple ORing of the distributed shares [3]. The gray scale image hidden in the shares is encoded with black & white pixels only & no colors pattern.

In case of image using white pixel, 4 sub pixel layout encoding this pixel as[0101] is used where 0 means black sub pixel and 1 means white sub pixel in the layout. This is done for both secret shares.

If the image uses a black pixel, 4 sub pixel layouts encoding this pixel as [0110] is used where 0 means black sub pixel and 1 means white sub pixel in the layout. This is done for both secret shares.

Clearly when the shares are at different users' sites; they don't reveal their secrets. However, when these are laid over each other correctly, the original image is recovered. No calculations are needed to do the same.

This basic idea was then applied in a (k, n) scheme by Naor and Shamir called threshold visual cryptography in which user having k qualified shares only will be used to obtain the original image. However, k out of n scheme is different from original scheme because in original scheme, all generated shares are used as the threshold whereas in (k,n) scheme threshold value k < n.

A probability based approach by deciding the contrast of recovered image through white pixels' density has been suggested by Ching-Nung Yang. Human Visual system can distinguish between the Black & white areas of gray scale image because the frequency of white pixels is more in the recovered image. The only disadvantage is that the poor pixel density results in picture getting degraded quality.

The problem with these Secret sharing schemes is that if any misfeasor leaks these shares to other party & the participants are not able to obtain the authorized shares. In this current scheme, we suppose participants are honest. Third Trusted Party (TTP) may be introduced to counter this problem. Our main idea is to construct a visual cryptography scheme in which each participant can do the verification of his share for authorization purpose. TTP does this authorization & gives the result. If the centre is not reliable; this scheme pays off without the increasing the expenses to implement this verification process.

In Extended verifiable VCS scheme, The TTP stores the shares of k-out-of-n & k+1-out-of-n threshold schemes simultaneously. The TTP could check if the shares are used & distributed by the digital signature of authority.

In the scheme, TTP need to stack the shares & applied with any k shares and give the result. Second problem to counter is pixel expansion.

Color based vcs using three primary colrs cyan, magenta & yellow could also be used. But this scheme suffers from large pixel expansion. This mandates high quality VC shares; which is very difficult. The scheme is secure, though. Changing the pixel density; this could be achieved.

PROBLEM STATEMENT:

The main statement of the problem is "Implementation of visual cipher based cipher scheme" for textual data. Already schemes are there for visual data but the same security as required for visual secret sharing scheme is to be developed for cipher techniques regarding 2 dimensional textual data. Code is proposed to be implemented in C language. There will be restrictions on graphics in C. Pixel layout has been created to have minimum distortion of image and least pixel expansion. Pixel expansion of the shares should be uniform. Reconstruction of the secret image should be as easy to obtain as it is to encrypt the same. Emphasis is on clarity. Simple mathematical formula has been used for stacking shares in code (XNOR). Researcher will analyze, evaluate and implement the model with various attacks through simulation study. Analyze the cipher model in terms of Quality, Contrast, Distortion level and Space required in its implementation.

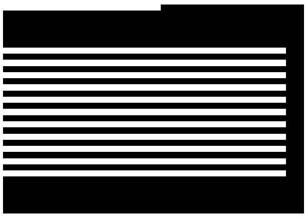
ACCOMPOLISHED WORK:

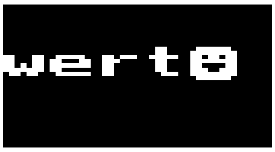
MODIFIED 2X2 VCS ALGORITHM:

Step 1: Draw an image in some area,let us say write text using outtextxy function.
Step 2: Store image coordinate area through getimage function.
Step 3: Generate share1 of sx2s size.
a)If image through getimage at (x,y) has White pixel;
store at(x’,y’) &(x’,y’+1) 1 & 0 respectively as per scheme 1 or 0 & 1 resp. as per scheme 2.
b) If image through getimage at (x,y) has Black pixel;
store at(x’,y’) &(x’,y’+1) 1 & 0 respectively as per scheme 1 or 0 & 1 resp. as per scheme 2.
Step 4: Generate share 2 of sx2s size.
a)If image through getimage at (x,y) has White pixel;
store at(x’’,y’’) &(x’’,y’’+1) 1 & 0 respectively as per scheme 1 or 0 & 1 resp. as per scheme 2.
b) If image through getimage at (x,y) has Black pixel;
store at(x’’,y’’) &(x’’,y’’+1) 0 & 1 respectively as per scheme 1 or 1 & 0 resp. as per scheme 2.
Note: 1 means to draw white pixel at specified coordinates. And 0 means to draw black pixel.
Step 5: Superimpose the two shares above by accessing first of the pixels at (x’,y’) and (x’’,y’’) through getpixel function and applying XNOR between them & subsequently printing the generated pixel at specified coordinates through putpixel; it generates the original image. A single share can’t produce the image.

EXPERIMENTAL RESULTS:

2-by-2 VCS scheme has been modified with reduced pixel expansion. The two shares Fig 2 (b) & Fig. 2 (c) of the image (Fig. 2(a)) have been taken in text mode treated as binary image. The decryption process involves stacking the two shares & applying XNOR operation to produce the original image in 2(d).

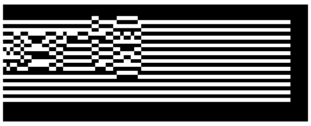




`

Fig. 2(b). Share 1

Fig. 2(a).Original Image.



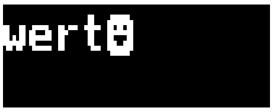


Fig. 2 (c) Share2

Fig. 2(d) Decrypted Image using XNOR Operation

This experiment can be easily expanded to 3-out-of-4 VCS. The scheme is perfectly secure and very easy to implement. The algorithm to implement the process is simple and does not require any complex mathematical operation.

CONCLUSION & FUTURE WORK:

The original schemes encodes every pixel from the original image into two sub pixels and expands pixel horizontally & may produce each sub pixel encoding column wise in Turbo C++ output window screen. The pixel could also expand vertically. Resulting in share size of s x 2s if the original image is of size s x s. This produces slight distortion in reconstructed image. This could be made better using the 4-subpixel layout with the size of shares being 2s x 2s with the original image of size s x s. This uniformity in pixel expansion (both horizontally & vertically) avoids the horizontal or vertical distortion in the recovered image. Not to forget that image extends 4 times larger than the original.

As a future work Code needs to be implemented for above modified 2-by-2 VCS algorithm in C language. Although further improvements needs to be done.

REFERENCES:

[1] Thomas Monoth, Babu Anto P. ICEBT 2010.Procedia Computer Science 2 (2010) 143–148..

[2] HAN Yanyan, YAO Dong, CHENG Xiaoni, HE Wencai inVVCS: Verifiable Visual Cryptography Scheme 2011 Seventh International Conference on Computational Intelligence and Security

[3] M. Naor and A. Shamir, Visual cryptography, in Advances in Cryptology (Lecture Notes in Computer Science), vol. 950. Berlin, Germany: Springer-Verlag, 1995.

[4] Gayathri , Dr T Gunasekran , Design of XOR based visual cryptography scheme, International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE) Volume 4, Issue 2, February 2015

[5] C.-N. Yang, New visual secret sharing schemes using probabilistic method, Pattern Recognit. Lett., vol. 25, no. 4, pp. 486 494, Mar. 2004.

[6] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, Visual cryptography for general access structures, Inf. Comput., vol. 129, no. 2, pp. 86 106, Sep. 1996

[7] Sandhya Anne Thomas, ME Scholar,Saylee Gharge, Associate Professor “Review on Various Visual Cryptography Schemes” International Conference on Current Trends in Computer, Electrical, Electronics and Communication (ICCTCEEC-2017)
1164 Authorized licensed.

AUTHOR

Abhishek Garg, has done B.Tech. (CSE) from AMU, Aligarh (U.P.), India in 2003. He has done M.Tech. (CSE) from Integral University, Lucknow. He is pursuing Phd. Computer Science & Engg. from Mangalayatan university, Aligarh. He has more than 18 years of teaching experience. His research interests are cryptography, C language etc.