International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 4 | Issue 3| ISSN : 2456-3307

Cheating Mechanism in Visual Cryptography a Novel Method with Efficient Halftoned Image with SBR Technique By Sealing The Algorithm

Ms. R. Nandhini[1], Mrs. S. Shanthi[2], Ms. A. Sivasankari[3]

[1]Research Scholar, Dept of Computer Science and Applications, D.K.M. College for Women (Autonomous), Vellore, Tamilnadu, India

[2]Assistant Professor, Dept of Computer Science and Applications, D.K.M. College for Women (Autonomous), Vellore, Tamilnadu, India

[3]Head of the Department (CS), Dept of Computer Science and Applications, D.K.M. College for Women (Autonomous), Vellore, Tamilnadu, India

ABSTRACT

The cheating is main issue while transferring the secret image against the owner. To avoid this Visual Cryptography novel method technique of cryptography is used. In this we divide secret images into multiple shares and are distributed to various entities. To get back the secret image we need all the shares. Using different operations we can reconstructed by superimposing these share. The pixel expansion and noise at output is a major drawback in Traditional. The major problem is cheating between shareholders cheating owners and between them. To avoid these limitation sealing algorithm with two application of visual cryptography (VC) are MIVC and EVC is used. The image will be changed into halftoned representation before sealing the algorithm. For this we are using SBR technique. The output overcomes common limitation likes pixel expansion and clarity of image along with this the system also provides a cheating prevention mechanism. Two secret image can be send at the same time by connecting them into halftonedrepresentations which are partitioned as totally three shares.

Keywords: Cheating, Shares, Halftoned Image, Pixel Expansion, Sealing Algorithm, Visual Cryptography.

I. INTRODUCTION

Visual Cryptography technique allows the encryption of an image without having any complex computations or cryptography knowledge. It is simply secrete sharing technique. In this secrete image are distributed to different entries. This technique initially proposed by Naor and Shamir in the year 1994. In this we need two transparent images. One image contains random pixels and another contains secret information. To retrieval the information, we need all the shares layers are to be overlapped. Because decryption is done only when all shares are overlap together, we get original image.

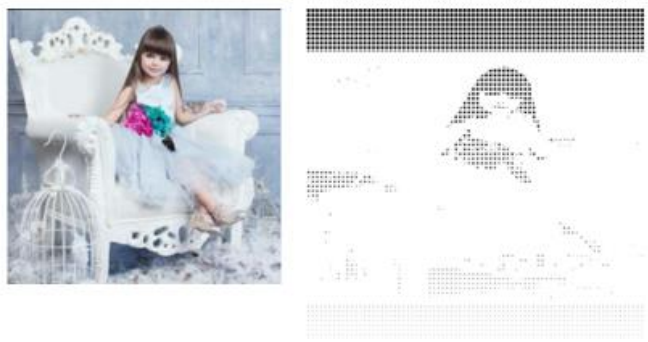


Figure 1. Basic Model of Visual Cryptography

In Visual Cryptography Biometric is an important security application. It has a Facial, Fingerprints, Signature image are used as secret key. To kept these images secret we distribute these images and shared. After different entities release the shares it overlapped to get back the secrete image. To solve the common and traditional drawbacks in Visual cryptography we use novel method. This includes image clarity, pixel expansion, cheating between shareholders and image content owner. Here two secret image are dived into three shares. Therefore three cover image are sealed into these shares for high security protection. For increase the security we can also add the pin number or password can be entered before the share creation and it should be identified correctly while overlapping of shares. Then only secret image is viewed to the user.

II. OBJECTIVE

In this the research is to test secure visual cryptography with halftoned images, do not require more pixels in the shared images. Better Image clarity after overlap secret image.

The overlap secret image was proposed with

To get secret image as better clarity and no loss of pixels.

As in the original image pixels is equal to the pixel in after overlapped secret image.

Apply cheating mechanism method used for secured transmission of secret image preventing from cheating.

III. PROPOSED METHOD

Novel Algorithm:

Step1: Read the input image.

Step 2: It is decomposed into three-share image based on RGB.

Step 3: The halftone technique is applied to these images to binary images.

Step 4: Read the share images or key images.

Step 5: Perform XOR operation between binary images obtained in halftone process.

Step 6: Repeat this process to every binary images.

Step 7: Now to overlap to get the original image will be back.

For receiver side process

Step 1: Read the encrypted image.

Step 2: Split the image.

Step 3: For each image perform these: Split the image into RBG.

Step 4: De-embedded the share image and each binary secrete image.

Step 5: Inverse the halftoning is performed to each image.

Perform Halftoning image process for each Pixel:

Halftoning: It is the process of converting images with greater amplitude resolution to lesser amplitude resolution.

Input: The matrix D cxd and a pixel with gray level g in input image I

Process [I]

For i=0 to c-1 do

If g=Dij then print black pixelat position (i,j)

Else print while pixel at position (i,j)

Output:halftoned image contain in the position of(i,j)

SBR Technique

Performs fully automatic mono-model registration of both images.

Step 1: Select image near the center of the dataset as a template image.

Step 2: Compute information and edge direction for each pixel.

Step 3: For each target image landmark pixel is assigned automatically.

Step 4: Compute edge information for landmark pixel

Step 5: Search matching pixel for landmark pixel in the template using kernel equation.

Embedded EVCs

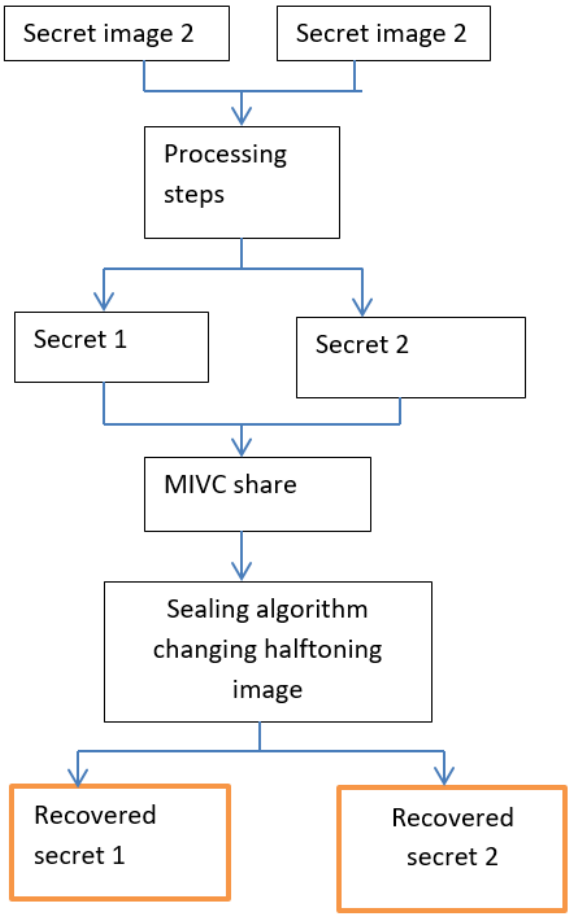
It contain two main steps
Step 1: n covering share will be generated.
Step 2: By embedding the corresponding vcs into the n shares.
First to generate the n covering shares for an access take gray-scale original share images and output n binary meaningful share.
Second use corresponding vcs to encode a secret image and then embedded shares that were generated.
Third decrypt the embedded shares them again to get original image.

Process

Input: n covering shares of (c0,c1) with pixel expansion and secret image I1
Step 1: Divide the covering shares into blocks that contain sub pixels
Step 2: Choose m embedding position in each block in n covering shares.
Step 3: For each black and white pixel in I1 randomly choose a share matrix M belongs to c1
Step 4: Embedded the m sub pixel of each row and column of the share matrix M into the m embedded position.
Output: n embedded share are e0,e1,e2…en-1

MIVC Share

Step 1: Two secrete image is masked.
Step 2: Rotate the pixel in the binary image of share 1 divided into two shares.
Step 3: Secret image became visible by superimposing the share 1 and share 2.
Step 4: It will combined with same share 3.



IV. CONCLUSION

For security issues while sharing secret images or keys is an important part. VCs is an efficient secret sharing technique where secret image into number of encrypted images. This work proposed sealing algorithm of novel method where secret image is divided into three shares. Share 1 and 2 generate secret image 1. Secret image 2 is obtained by rotating pixels of binary image in share 1 and combined the same with share 3. It prevents cheating between shareholders and owners. It will overcome loss of image clarity as well as pixel expansion as in the same ratio in the original image.

V. REFERENCES

[1] NazaninAskari, Howard M. Heys, Member, IEEE, and Cecilia R. Moloney, Member , IEEE "Novel Visual Cryptography Schemes without Pixel Expansion for halftone images" IEEE trans. 2014.

[2] Xiatian Wu and Wei Sun, "Extended Capabilities for XOR based Visual Cryptography" in IEEE 2013.

[3] Young-Chang Hou, Shih-Chieh Wei and Chia-Yin Lin "Random-Grid –Based Visual Cryptography" Schemes in the year of2013 in IEEE,2013.

[4] Pallavi V. Chavan and Dr. Mohammad Atique, "Design of Hierarchical Visual Cryptography" in IEEE, 2012.

[5] Z.Zhou, G. R. Arce, and G. D. Crescenzo, "Halftone Visual Cryptography" IEEE Trans. Image Process., vol 15, no 8, pp. 24412453, Aug 2006.

[6] A. Ross and A. A. Othman, "Visual cryptography for biometric privacy" IEEE Trans Inf Forensics Security, vol. 6, no 1, pp.7081, Mar. 2011.