International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 4 Issue 6, June-2015, pp: (205-209), Impact Factor: 1.252, Available online at: www.erpublications.com

Design for Region Incrementing Visual Cryptography Scheme

Poonam

Department of Computer Science, R, N. College of Engineering & Management, Rohtak, Haryana, India

Abstract: **A Region Incrementing Visual Cryptography Scheme (RIVCS) deals with the sharing of an image consisting of multiple regions with different secrecy levels, which can be incrementally revealed as the number of shares increases. It is a method of encrypting a secret image into shares such that stacking a sufficient number of shares reveals the secret image. Shares are usually presented in transparencies. Visual Cryptography Scheme (RIVCS) can achieve the minimum pixel expansion and the maximal contrasts. An efficient construction for RIVCS using linear programming is presented in this paper. The proposed integer linear program aims at the minimization of the pixel expansion under the constraints for being a RIVCS.**

Keywords: **Embedded region incrementing visual cryptography scheme, halftone, tampering, shares.**

I. INTRODUCTION

Various A Region Incrementing Visual Cryptography Scheme (RIVCS) deals with the sharing of an image consisting of multiple regions with different secrecy levels, which can be incrementally revealed as the number of shares increases. It is a method of encrypting a secret image into shares such that stacking a sufficient number of shares reveals the secret image. Shares are usually presented in transparencies [1]. Visual Cryptography Scheme (RIVCS) can achieve the minimum pixel expansion and the maximal contrasts. An efficient construction for RIVCS using linear programming is presented in this paper. The proposed integer linear program aims at the minimization of the pixel expansion under the constraints for being a RIVCS.[3]

II. EXISTING SYSTEMS

Existing visual cryptography schemes that are used for data hiding have a security hole in the encrypted Share file. If the share images are hacked, the hacker can tamper the data that is hidden and hence can disturb the entire technique. In the existing, there is no optimized secured way to access the secret hidden data and the data that are stored in databases.

III. THE PROPOSED SYSTEM

This paper concentrates on the task to provide security features for database system in terms of visual cryptography schemes. In proposed system, to prevent the accessing of data in database, the security is enhanced in three phases using visual cryptography. First, an image is split into n encrypted shares using algorithm by the fact that a pixel can be split into sub pixels. Second, in order to avoid hacking of shared image, employ password protection for each share using Extended Embedded algorithm and simple Arithmetic Encoding compression technique which compresses the pass code. Third, rearranging of pixels of shared images are performed by overlaying process to obtain the access to the protected database.

A. Advantages of the Proposed System

- An efficient construction for RIVCS using linear programming is developed.
- The proposed integer linear program aims at the minimization of the pixel expansion under the constraints for being a RIVCS.
- Experimental results demonstrate the feasibility, applicability, and flexibility of the construction. The pixel expansions and contrasts derived from the scheme are also better than the previous results.

International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 4 Issue 6, June-2015, pp: (205-209), Impact Factor: 1.252, Available online at: www.erpublications.com

IV. DESIGN AND ARCHITECTURE

A. System Architecture

The architecture of the proposed system is shown in Figure 2.

B. Modules

The following modules were used for the system:

1. Sender

User provides a secret image and outputs of Original shares image which is relevant for the secret.
There are two conditions:

- Any qualified subset of shares can recover the secret image
- Any forbidden subset of shares cannot obtain any information of the secret image other than the size of the secret image.

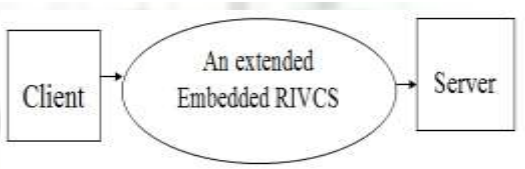

Fig. 1: Sender Module

2. Halftone Pattern

The original image with only k shares out of n shares is obtained, and then, all the 'n' image shares are necessarily overlaid when all the image shares that are overlaid are authenticated to be from the same original image. VCS share with transparent pixels and pixels from the cover images. RIVCS uses half toning techniques, and hence can treat grey scale input share images. This method makes use of the complementary images to cover the visual information of the share images.

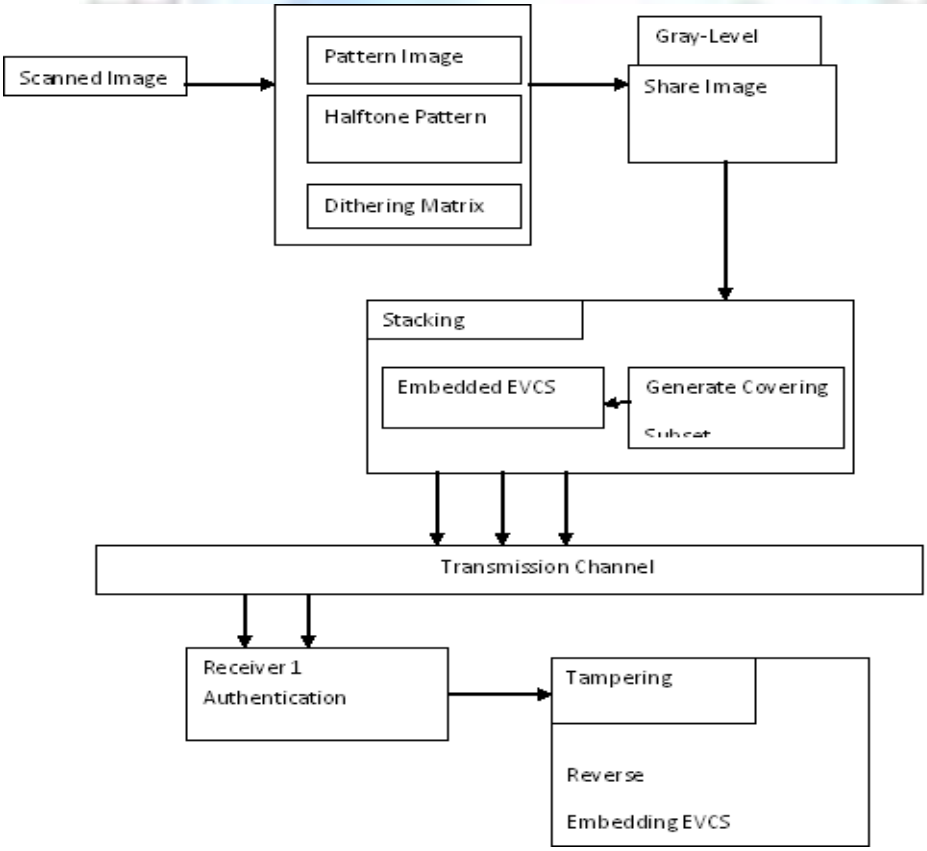

Fig. 2 Architecture diagram for the proposed system

By using Patterning, dithering matrix makes use of a certain percentage of black and white pixels, often called patterns, to achieve a sense of grey scale in the overall point of view.

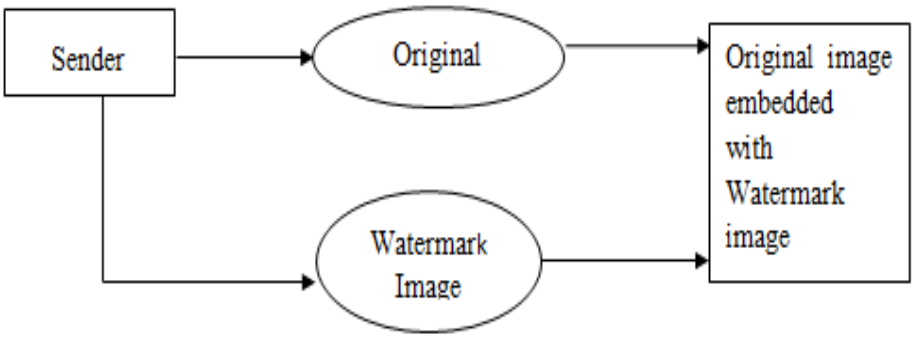

Fig. 3 : Halftone Pattern Flow Chart

3. Embedded RIVCS

Embedded RIVCS encode a secret image, the dealer takes grey-scale original share images as inputs, and converts them into covering shares which are divided into blocks of sub pixels. Embedded RIVCS contains three main steps:

- Generate covering shares.
- Generate the embedded shares by embedding the corresponding VCS into the 'n' covering shares.
- Region Incrementing Visual Cryptography Scheme (RIVCS) can achieve the minimum pixel expansion and the maximal contrast Integer linear program aims at the minimization of the pixel expansion under the constraints for being a RIVCS. [2]

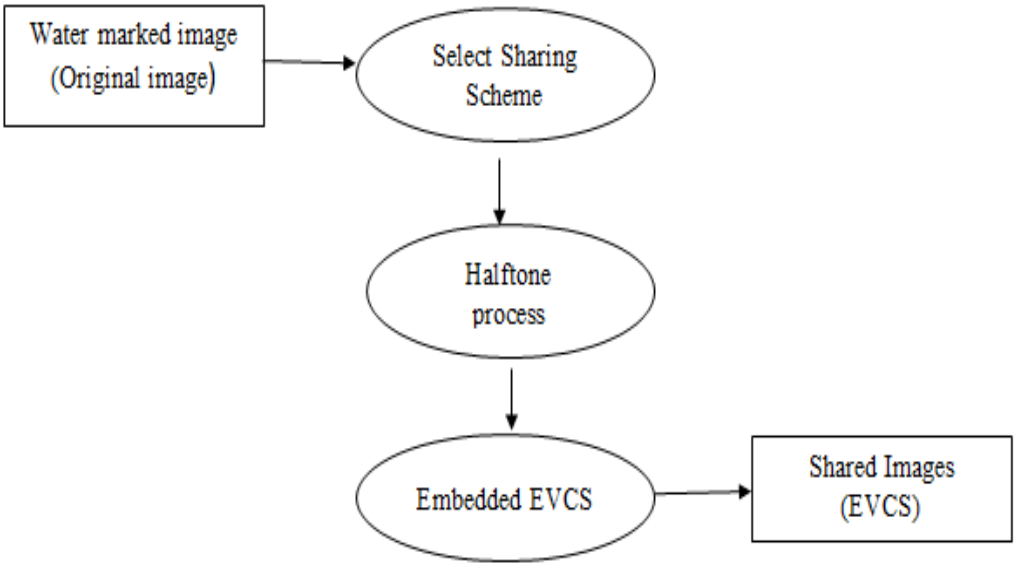

Fig. 4: Embedded RIVCS Flow Chart

4. Recipient/Authentication

Authentication has been verified by using Hash Authentication Code algorithm. Authorized user (Recipient) only is able to access the image, transmitted from Sender.

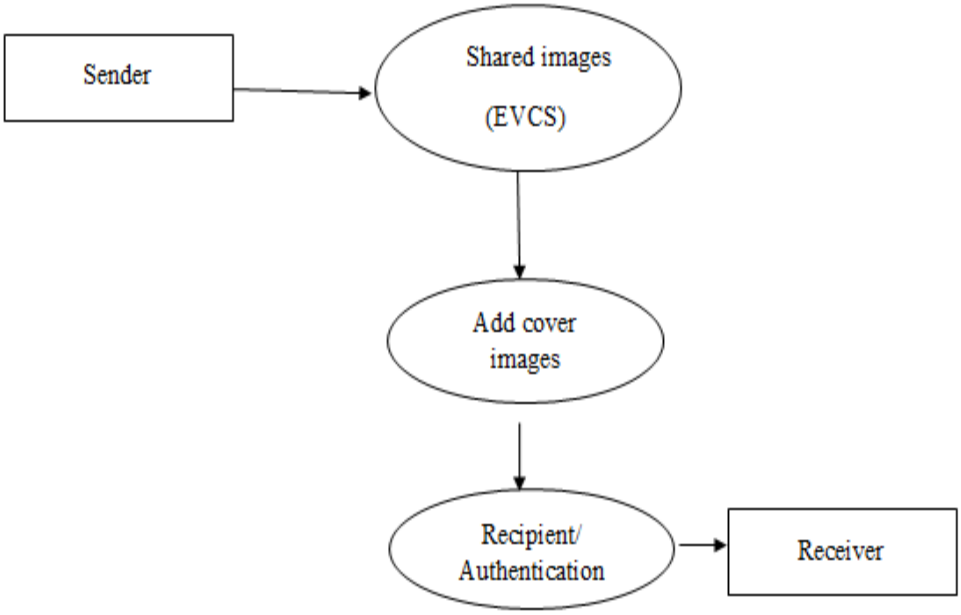

Fig. 5: Recipient/Authentication Flow Chart

5. Tampering

To detect whether or not a digital content has been tampered with in order to alter its semantics, the use of multimedia hashes turns out to be an effective solution. The hash is used to estimate and prevent the mean square error distortion between the original and the received image. At the cost of additional complexity at the decoder, the proposed algorithm is robust to moderate content-preserving transformations including cropping hash decoding.

C. Proposed Algorithm

The following process is used for implementation:

- Select the grey scale image.
- Apply the LZW compression technique for the grey scale image.
- Preparing the dictionary for the grey scale images.
- In dictionary replaces strings of characters with Single codes.
- Calculations are done by dynamic Huffman coding.
- In compression of grey scale image select the secret Information pixels.
- Then generation of halftone shares using error diffusion method.

CONCLUSIONS

The shares of the proposed scheme are meaningful images, and the stacking of a qualified subset of shares will recover the secret image visually. Two methods to generate the covering shares, and proved the optimality on the black ratio of the threshold covering subsets. Here a method to improve the visual quality of the share images is proposed. Furthermore, the construction is flexible in the sense that there exist two trade-offs between the share pixel expansion and the visual quality of the shares and between the secret image pixel expansion and the visual quality of the shares. This thesis concentrates on the task to provide security features for database system in terms of visual cryptography schemes. In the proposed system, to prevent the accessing of data in database, the security is enhanced in three phases using visual cryptography.

ACKNOWLEDGEMENTS

I would like extend my thanks and gratitude to all the referenced authors.

REFERENCES

[1]. Droste.S, (1996) "New results on visual cryptography," in Proc. Advances Cryptography, LNCS 1109, pp. 401–415.
[2]. Zhi Zhou, Member, IEEE, Gonzalo R. Arce, Fellow, IEEE, and Giovanni Di Crescenzo, (august), 2006,"Halftone Visual Cryptography" IEEE transactions on image processing, vol. 15, no. 8
[3]. Wang, R.Z.[Ran-Zan], "Region Incrementing Visual Cryptography", SPLetters(16), No. 8, August 2009,pp. 659-662.