Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 5, Issue 4, April-2018

SECURED IMAGE SHARING USING VISUAL CRYPTOGRAPHY

GA. Lakshmi[1], F. Lubna Kousar[2], S. Mukesh[3],

[1]*Pondicherry Engineering College*, godesslak471@gmail.com

[2]*Pondicherry Engineering College*, lubnaksr1997@gmail.com

[3]*Pondicherry Engineering College*, mukeshsubburayan@gmail.com

ABSTRACT- Main benefit of this scheme is mathematical computation complexity is reduced to visual cryptographic(VC) techniques. Each participant holds a transparency. Most of the previous research work on visual cryptography focuses on two parameters: large pixel expansion and contrast. The number of sub pixels (m) for converting each secret pixel, referred to as the pixel expansion, is the smaller the enhanced to reduce the share size. The pixel expansion and relative contrast are the most critical measurements to assess the effectiveness of a visual cryptography. In this paper, we studied VC in addition to Deterministic Visual Cryptography (DVCS) can achieve the minimum pixel expansion and the maximal contrast. We develop a novel and efficient construction for Random Grid and DVCS in this paper.The proposed Visual Cryptograms of Random Grids model and deterministic model aims at the minimization of the pixel expansion and maximal contrasts for individual VC. The Experimental results demonstrate the feasibility of our construction. The pixel expansions and contrasts derived from our scheme are also better than the previous results.

I. Introduction

Visual cryptography is a cryptographic method that allows visual information to be encrypted in such a way that decryption becomes the job of the end user. Visual Cryptography is a wide area of study used in data hiding, securing images, color imaging, multimedia and other such fields. Visual Cryptography occurs in the field of data hiding used in cybercrime, file formats etc.

Naor and Shamir introduced a very interesting and simple cryptographic method called visual cryptography to protect secrets. Basically, visual cryptography has two important features. The first feature is its perfect secrecy and the second is its decryption method which requires no complex decryption algorithms . It uses only human visual system to identify the secret the stacked image of some authorized set of shares. Therefore, visual cryptography is a very useful way to protect secrets when computers or other decryption devices are not available. The simple decryption method is the cause that attracts many researchers to make further detailed enquiries in this research area. Nowadays, many related methods concerning the theory and the applications of visual cryptography are proposed. An extended visual cryptography scheme (EVCS) was proposed by Ateniese et al.Extended visual cryptography schemes permits the construction of visual secret sharing schemes within which the shares are meaningful as opposed to having random noise on the shares. After the sets of shares are superimposed, this meaningful information disappears and the secret is recovered. This is the basis for the extended form of visual cryptography. The image size invariant visual cryptography was proposed by Ito et al.

II. Related Work

In [1] the author has discussed about Region incrementing visual cryptography (RIVC) is referred to as a new type of multi-secret VC. RIVC defines s layers and takes s secrets, and then embeds each secret into each layer. The layers are defined by the number of participants; for example, let two secrets and two layers be S2,S3 and L2,L3 in 2-out-of-3 RIVC, where any two participants in L2 can recover S2 and three in L3 can recover S2,S3. However, there is another multi-secret VC, called fully incrementing visual cryptography (FIVC), which also has the layers, but only one se3cret Si will reveal in one layer Li

In [2] the author has discussed about an HVCS construction method with minimum auxiliary black pixels (ABPs) distributed homogeneously, which is realized via embedding secret image into meaningful shares in the halftoned processing of the cover images by error diffusion. Secret information pixels (SIPs) are fixed in parallel and separated maximally from each other before the halftoned processing. The proposed scheme obtains admirable visual quality and some preferable advantages compared with related meaningful VC schemes (VCSs).

In [3] the author has discussed about analysis the definition of cheating prevention and propose a new authentication based cheating prevention scheme. This scheme is constructed with Naor–Shamir's VC scheme. Finally, we give the security analysis to prove that the proposed scheme is immune to cheating. The limitations in this paper is that the total number of subpixels for sharing a pixel is less.

In [4] the author has the proposed of n-level RIVC scheme, the content of an image S is designated to multiple regions associated with n secret levels, and encoded to n+1 shares with the following features: (a) each share cannot obtain any of the secrets in S, (b) any t (2lestlesn+1) shares can be used to reveal t-1 levels of secrets, (c) the number and locations of not-yet-revealed secrets are unknown to users, (d) all secrets in S can be disclosed when all of the n+1 shares are available, and (e) the secrets are recognized by visually inspecting correctly stacked shares without computation

In [5] the author has discussed about a more secure scheme is given to solve the cheating problem without extra burdens by adopting multiple distinct secret images. Moreover, for sharing these secret images simultaneously, the share construction method of visual cryptography is redesigned and extended by generic algorithms. Finally, the results of the experiment and security analysis show that not only the proposed scheme is more secure in comparison with the two previous cheating prevention schemes in the literature, but extra burdens are also eliminated.

III. Methodology

SENDER

User provides a secret image and outputs of Original shares image which relevant for secret.

We can satisfy with the 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.

HALFTONE PATTERN

We can obtain the original image with only k shares out of n shares, 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.

MSVCS share with transparent pixels and pixels from the cover images.

EMBEDDED MSVCS

Embedded MSVCS encode a secret image , the dealer takes grayscale original share images as inputs, and converts them into covering shares which are divided into blocks of sub pixels.

Our embedded MSVCS contains three main steps:

- Generate covering shares.
- Generate the embedded shares by embedding the corresponding VCS into the 'n' covering shares.
- Multiple-Secret Visual Cryptographic Schemes (MSVCS) can achieve the minimum pixel expansion and the maximal contrasts.
- Integer linear program aims at the minimization of the pixel expansion under the constraints for being a MSVCS.

STACKING (Covering Subsets)

The stacking results of the qualified shares are all black images, the information of the original share images are all covered. The stacking results are not necessarily to be all black images. The covering shares have the advantage it's a qualified subsets of stacked. All the information of the patterns in the original share images is covered. Hence the visual quality of the recovered secret image is not affected.

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.

Hash-based Message Authentication Code (HMAC) is a message authentication code that uses a cryptographic key in conjunction with a hash function

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 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.

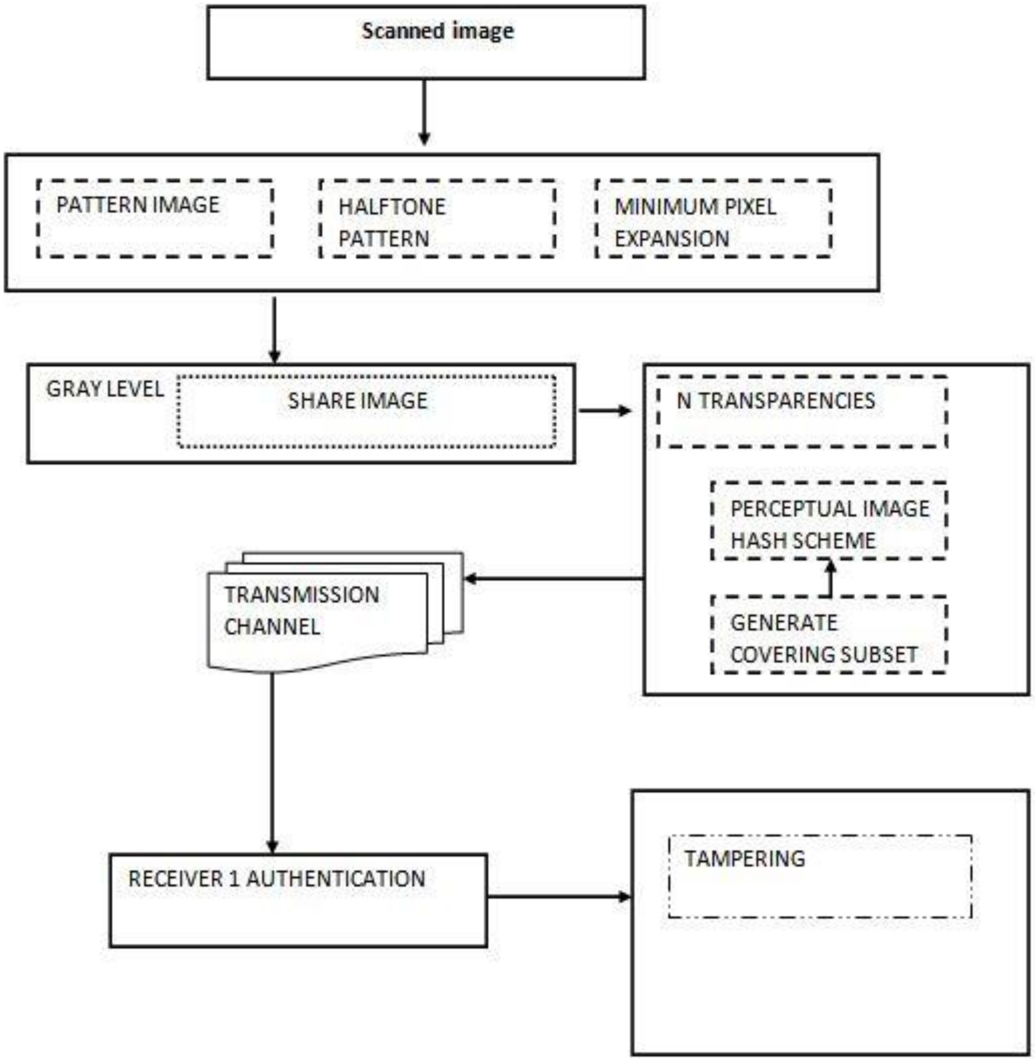

Fig 1. System Architecture

IV. CONCLUSION

The proposed Visual Cryptograms of Random Grids model and General Access Structures aims at the minimization of the pixel expansion and maximal contrasts. Image hacking is prevented by encoding a secret passcode in each shares by which authenticated users can decrypt the image.The proposed Visual Cryptograms of Random Grids model and deterministic model aims at the minimization of the pixel expansion and maximal contrasts for individual a VC. The Experimental results demonstrate the feasibility, applicability, and flexibility of our construction. The pixel expansions and contrasts derived from our scheme are also better than the previous results.The idea is to convert the written material into a binary image and encode this image in to n shadow image it is also called as shares of images. The decoding only requires selecting some subset of these n shadow images, making transparencies of them and stacking them on top of each other. Main advantage of this scheme is mathematical computation complexity is reduced to visual cryptographic techniques.

V. REFERENCES

[1] Yu-Chi Chen "Fully Incrementing Visual Cryptography from a Succinct Non-Monotonic Structure", , IEEE Transactions on Information Forensics and Security, DOI 10.1109/TIFS.2016.2641378, 19 December 2016.

[2] X. Yan, S. Wang, X. Niu, and C.-N. Yang, "Halftone visual cryptography with minimum auxiliary black pixels and uniform image quality," Digital Signal Processing, vol. 38, pp. 53–65, 2015.

[3] Y. C. Chen, D. S. Tsai, and G. Horng, "A new authentication based cheating prevention scheme in Naor-Shamir's visual cryptography," Journal of Visual Communication and Image Representation, vol. 23, pp. 1225–1233, 2012.

[4] R.-Z. Wang, "Region incrementing visual cryptography," IEEE Signal Processing Letters, vol. 16, no. 8, pp. 659–662, 2009.

[5] D. S. Tsai, T. H. Chen, and G. Horng, "A cheating prevention scheme for binary visual cryptography with homogeneous secret images," Pattern Recognition, vol. 40, pp. 2356–2366, 2007.

Author Biography

GA . Lakshmi pursuing B.Tech degree in the Department of Information Technology in Pondicherry Engineering College.

F. Lubna Kousar pursuing B.Tech degree in the Department of Information Technology in Pondicherry Engineering College.

S. Mukesh pursuing B.Tech degree in the Department of Information Technology in Pondicherry Engineering College.