Computers and Electrical Engineering 000 (2017) 1–12

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Extended visual cryptography techniques for true color images[☆]

Kirti Dhiman[*], Singara Singh Kasana

Computer Science and Engineering Department, Thapar University, Patiala, Punjab-147004, INDIA

ARTICLE INFO

Article history:
Received 28 April 2017
Revised 17 September 2017
Accepted 19 September 2017
Available online xxx

Keywords:
Secret sharing
Visual cryptography techniques
Extended visual cryptography techniques
RGB decomposition
RSA
DES

ABSTRACT

In this work, two extended visual cryptography techniques for sharing color images are proposed. Three meaningful shares are generated in both techniques using a block size of 5 × 5 corresponding to each pixel of original secret image. First proposed technique is (3, 3)-*EVCT* in which first share contains *R* component, second contains *G* component and third contains *B* component of the secret image. All three shares are required to reconstruct the original secret image on the receiver side. Second technique is (2, 3)-*EVCT* in which any 2-out-of-3 shares are needed to recover the original secret image on the receiver side. Out of these shares, first share contains the *RG* components, second contains *GB* components and third contains *RB* components of the secret image. All shares in both techniques are meaningful as they contain the cover images along with the information of the original secret image. These shares are made meaningful in order to increase the security and to avoid the suspicion that something is hidden there. The proposed techniques are lossless in nature and are less complex. The dimensions of the original secret image, cover images, regenerated secret image are same. The effectiveness of the proposed techniques have been shown by comparing their results with the results of the existing techniques on the basis of various parameters.

1. Introduction

Data exchanged over the Internet is in the form of images, audio, video, text, handwritten text, graphic objects, animations, *etc*. The media used in data exchange is unreliable and insecure. Security of the digital media has become an important topic as it can be copied and modified easily. Cryptography is one of the techniques, which can be used for security of exchanged data. It ciphers the plain text to make it as cipher text, which is actually communicated through the communication media so that intruders even if obtain the cipher text do not be able to decipher the original information hidden within the cipher text. The examples of cryptography are Data Encryption Standard (*DES*), triple DES (*3DES*), Advanced Encryption Standard (*AES*), Blowfish in which encryption and decryption are done by same key. *RSA* is another popular algorithm for asymmetric cryptography in which encryption and decryption are done using different keys.

Images are a vital form of multimedia contents, which are extensively exchanged over the Internet. So, there should be a secure and simple way to exchange images through any unsecured medium. In order to protect the image contents, Naor and Shamir [13] proposed Visual Cryptography (VC). Using VC, a user can identify confidential data without any computation.

[☆] Reviews processed and recommended for publication to the Editor-in-Chief by Guest Editor Dr. J. Papa.

[*] Corresponding author.
E-mail addresses: kdhiman_me15@thapar.com, kdhiman_me15@thapar.edu (K. Dhiman), kasana_s@yahoo.com (S.S. Kasana).

https://doi.org/10.1016/j.compeleceng.2017.09.017

In (*k*, *n*)-VCT, *n* shares (shadow images) of the secret image are generated during encryption and are sent through any untrusted medium. Out of *n* shares, any *k* shares are just stacked/superimposed (logical *OR* operation or *AND* operation depending upon which color is considered which bit) at the recipient's side to get the original secret image back. Any less than *k* shares would not regenerate the original secret image.

The advantage of *VCT* over other cryptographical techniques used for other multimedia content like text, audio, video is its decryption process, which does not involve any complex calculations and computations but can only be done by Human Visual System (*HVS*) *i.e.* human eye. Furthermore, no key is required for encryption/decryption in *VCT* as in other cryptographic techniques.

The two main aspects of the *VCT* are contrast and security. Researchers have been proposing various techniques to increase the contrast and security for many years. The researchers proposed that the logical *XOR* operation instead of *OR* operation could improve the contrast in case of binary images.

The shares generated in *VCT* are random-noise like shares. *EVCT* [2–4] was proposed to increase the security of shares by making the shares meaningful in order to reduce the suspicion that something is hidden there. So, the shares in *EVCT* contain the hidden information of the original secret image along with the cover image. The cover image can be the binary image, gray-scale image or the colored image.

Moreover, the other way *VC* can be performed is that any subset of shares, which are generating the original secret image is called qualified subset and the subset that is not generating the original secret image is called forbidden subset. Now-a-days colored images are much in use. Applying *VCT* on colored images is a complex procedure especially, on true color images. In this paper, two *EVC* Techniques are proposed *i.e.*, (3, 3)-*EVCT* and (2, 3)-*EVCT* for true colored images. In both the techniques, shares store the *RGB* component's information of the original secret image. The generated shares would be meaningful as the cover images would be embedded in the shares along with the *RGB* information. The encryption/decryption procedure is simple as compared to existing techniques.

The paper has been organized in sections as: Section 2 contains related work, motivation and contribution of the proposed work. In Section 3, proposed techniques have been discussed. Experimental Results and their discussion have been elaborated in Section 4. Conclusion and future work have been discussed in Section 5.

2. Related work, motivation and contribution of the proposed work

In this section, literature survey related to proposed work, motivations and contributions are discussed.

2.1. Related work

VC for binary images was initially proposed by Naor and Shamir [1]. Initially, the scheme was implemented as (2, 2)-*VCT* in which 2-out-of-2 shares are needed to recover the original secret image. The generated shares are random-noise like shares. Single share can't reveal any information about the original secret image. Each pixel in the original secret image can be expanded to any number of sub-pixels. After expansion, each pixel would be having a total number of *m* sub-pixels.

In [5], Koga and Yamamotq proposed the (*k*, *n*)-VCT for gray-scale and colored images by using lattice based concept. Any colored image with *J* distinct colors can be shared by using their technique. Mathematically, (*k*, *n*)-VCT for colored images having *J* colors is defined as the group of *J* subsets in the *n*th Cartesian product of finite lattice considered as the pixels corresponding to the shares and stacking of the shares is mathematically done by performing the Least Upper Bound (*LUB*) operation on the elements of the lattice. Hofmeister et al. [6] extended Noar and Shamir technique by using linear programming to enhance the contrast of the output images.

Ateniese et al. [4] enhanced the security feature in the *VC* by making the shares meaningful thereby naming the technique as Extended Visual Cryptography Technique (*EVCT*). The shares in *EVCT* have a cover image embedded in them to avoid suspicion that something is concealed there. Authors proposed (2, 2)-*EVCT* for binary images in which each white pixel from cover image is expanded to 2-white-2-black sub-pixels block and each black pixel from cover image is expanded to 1-white-3-black sub-pixels block in every share. When the shares are stacked, the resultant image would be having 1-white-3-black sub-pixels blocks corresponding to the white pixel of the original secret image and 4-black sub-pixels block corresponding to the black pixel of the original secret image. The shares have reduction in contrast by 50% while the regenerated original secret image has 75% contrast reduction.

Hwang and Chang [7] customized Ateniese's *EVCT* model by taking each pixel from original image as 3 × 3 sub-pixels block in share images. The shares are having 5 and 7 black sub-pixels corresponding to the white and black pixels of the cover image and 7 and 9 black sub-pixels corresponding to the white and black sub-pixels of the original image.

Chang [8] proposed a technique in which a gray-scale image is stored in different shares. The size of the shares does not vary as the number of colors in image changes. The implementation complexity is less than the other techniques. Hou [21] proposed three different (*k*, *n*)-*VCTs* for gray-scale and colored images using halftoning technique and color decomposition method. Their technique is also applicable to the binary images. Chang et al. [9] extended the technique given in [10] for the colored images, but the contrast is 2/9 of the original image which was even worse than with the Ateniese's technique (1/4).

In [11], Chao and Lin proposed a (2, 3)-threshold *VCT* using *CMY* color decomposition method and error injection. The true color 24-bits original secret image is converted into three 1-bit halftone images *C*, *M* and *Y* or a single 3-bit *C-M-Y*