Advances in Computer Science and Information Technology (ACSIT)
p-ISSN: 2393-9907; e-ISSN: 2393-9915; Volume 6, Issue 3; July-September, 2019, pp. 155-157

http://www.krishisanskriti.org/Publication.html

Region Based Cryptography: An Upgraded Algorithm for Visual Based Cryptography for Secret Image Hiding

Irfan Jalal Bhat [1], Dr. Raghav Mehra [2], Dr. Amit Kumar Chaturvedi[3]

[1]Research Scholar, Computer Application, B. U. Ajmer (India)
[2]Associate Professor & Dean Student Welfare Bhagwant Institute of Technology, Muzaffarnagar (India)
[3]Assistant Professor MCA Department Govt. Engineering College, Ajmer Rajasthan (India)
E-mail: [1]irfanbhatphd@gmail.com, [2]amit0581@gmail.com, [3]raghav.mehrain@gmail.com

Abstract—*Visual Cryptography depends on cryptography where n pictures are encoded such that lone the human visual framework can decode the concealed message with no cryptographic calculations when all offers are stacked together. This paper presents an improved algorithm based on Chang's and Yu visual cryptography scheme for hiding a colour image into multiple colour cover images. This plan accomplishes lossless recuperation and diminishes the clamor in the spread pictures without including any computational unpredictability.In this paper we also show some of the concept about how these algorithm help in secret sharing image.*

Keywords: *Image processing, visual Cryptography, secret sharing, hiding, region based cryptography.*

Introduction

The main instantiation of VC realizes a cryptography protocol called secret sharing (SS). In a conventional SS scheme, a secret image is shared among n participants in such a way that subsets of quali_ed participants can pull their shares and recover the secret but subsets of forbidden participants can obtain no information about it. Here, both the sharing phase and the reconstruction phase involve algorithms that are run by computers (specially, a dealer runs a distribution algorithm and a set of quailed parties can run a reconstruction algorithm). The surprising novelties of a VSS scheme are in representing data as images and in an elementary realization of the reconstruction phase, consisting of just viewing the image obtained after stacking transparencies. VSS schemes inherit all applications of conventional SS schemes; most notably, access control. As an example, consider bank vaults that must be opened everyday by have tellers, but for security purposes it is desirable not to entrust any two individuals with the combination. Hence, a vault-access system that requires any three of the have tellers may be desirable. This problem can be solved using a 3-out-of-5 threshold scheme. In addition to access control, VSS schemes can be applied to a number of other cryptographic protocols and applications using conventional SS, such as threshold signatures, private multiparty function evaluation, electronic cash, and digital elections. Another quite intriguing instantiation of VC schemes realizes VSS with innocent-looking images as shares. This version of VSS has applications to a multiparty variant of steganography. In a steganography scheme, a user A sends an innocent-looking image to another user B, in such a way that B can recover some hidden images, but no observer of the communication between A and B even suspects that the communication contains some hidden images. Cryptography plays a very vital enabling role in our modern computing infrastructure. Almost all real-world applications require keys (such as passwords) for the purposes of con_dentiality, authentication, and nonrepudiation. The strength of such cryptographic applications is based on the secrecy of a key. Therefore, the loss of a key can lead to disastrous consequences. Thus, many cryptographers have tackled the following problem: Suppose a secret s (a key) is divided into n > 1 parts (called secret shares) and it satisfies these properties:

1. The secret key s can be easily restored from k (k _ n) shares.
2. The secret key s cannot be restored from k - 1 (or less) shares.
3. The size of each share is not more than the size of the secret key s.

Such a scheme is referred to as a (k; n) threshold cryptography scheme or a secret sharing system[2][17]. It provides a backup mechanism to the secret key and it provides protection against the loss of a key. Secret sharing is also regarded as a mechanism to transfer secret information by public channels in cryptography [4]. Blakley based his secret sharing scheme on hyperplanes [17] and Shamir provided a solution based on the Lagrange interpolation [2]. Asmuth and Bloom scheme is based on the Chinese Remainder Theorem [5]. The details of these methods are available in [1] [12]. These traditional secret sharing schemes primarily concentrate on bit strings and

do not take the speci_c content of these bits into account. However, with the increasing emphasis on security and digital rights management of multimedia data, the connection between multimedia and cryptography is becoming stronger. In this context, we present our novel ideas on color image sharing in which we utilize the concept of secret sharing from cryptography and employ it to protect a secret color image. As we shall see, the ideas cannot be directly applied so we need to take into account that the data under consideration describes color images and is not any generic bit stream. In our scheme, a secret color image is divided into n shares. Each share is an innocuous image totally unrelated to the secret image. We utilize k (or more) shares in order to perfectly reconstruct the secret image. However, having access to k -1 (orless) shares will not reveal the secret color image. We envisage several useful applications for a color image sharing scheme. Suppose we have a secret color image that we desire to protect. If we employ traditional cryptographic techniques, then we need to encrypt the image and store the image on a secure server. We then need to pay attention on the security of the key used for encryption. This server would then become a single focus of attack from a potential adversary. However, with an image sharing scheme, we can divide the information in the image into several shares and keep them on separate servers. This would allow for a lot more redundancy in the protection since breaking one server will not reveal the secret image. Another application would be that of data hiding. Suppose we would like to transmit a secret image over a noisy and insecure channel. We could divide the image information into several shares that are basically innocuous images. These images could be transmitted and at the other end, the secret image could be reconstructed from the threshold number of shares. Another useful application would be that of a military command and control system based on the Clark-Wilson security model [11]. Suppose we want the battlefield plans to be made only if k out of n commanders agree. In which case, we could divide the battle terrain map into n shares and distribute it to the commanders. Only if k of them get together can they restore the terrain map and agree to a battle plan.

Chang's Algorithm (Progress)

Chang et al. proposed in 2002 another mystery shading picture sharing plan [1] dependent on altered visual cryptography. The proposed methodology utilizes significant shares (spread pictures) to conceal the shaded mystery picture and the recuperation procedure is lossless. The plan characterizes another stacking activity (XOR) and requires a grouping of arbitrary bits to be produced for every pixel. Chang's plan can be summed up to a n out of n approach as restricted to Chang Tsai's plan introduced already.

Secreting Algorithm

The For a 2 out of 2 plan, the development can be depicted by an accumulation of 2x9 Boolean grids C. In the event that a pixel with shading k=(k1k2… k8)2 should be shared, a seller haphazardly picks a number r somewhere in the range of 1 and 9 comprehensively just as one lattice in C. The development is viewed as substantial if the following conditions are fulfilled:

$k_i = S_{1\,j} + S_{2\,j}$ .....(a)

where $k_i = S_{1\,j} + S_{2\,j}$ and $j = \begin{cases} i & \text{if } i<r \end{cases}$

Note that the number of 1's in the first row of S must exceed the number of 0's by one.

Steps of the Algorithm

- Take a colored secret image I_{HL} of size *HxL* and choose any two arbitrary cover images O^1_{HL} and O^2_{HL} of size *HxL*
- Scan through IHL and convert each pixel Iij to an 8-bits binary string denoted as $k= (k1k2…k8)_2$
- Select a random integer r_p, where $1 \le r_p \le 9$ for each pixel Iij
- According to r_p and k for each pixel, construct S to satisfy equation (a)
- Scan through O^1 and for each pixel of color $k^1{}_p$, arrange the row "i" in S as a 3x3 block $B^1{}_p$ and fill the subpixels valued "1" with the color $k^1{}_p$

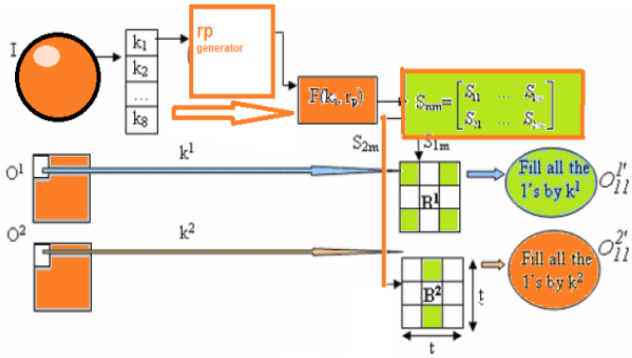

Fig. 1: Chang and Yu's secret sharing algorithm flowchart

Hiding Algorithm

Before subpixel expansion, add one to all pixels in the over images and limit their maximum value to 255. This ensures that no "0" valued pixels exist in the images. When the images are expanded, replace all the 0's in S_0, S_1text. byvalues corresponding to k_1-*1* in B1 and k_2-*1* in B_2 (Figure 2) in its place of leaving them transparent. Also, adjust all pixel values to be between 0-255

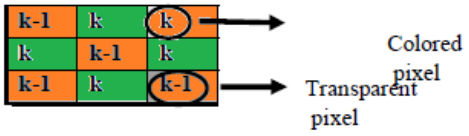

Fig. 2: Improved block subpixel expansion technique

Conclusion

This paper exhibited another strategy dependent on Chang et al. calculation [5] to shroud a shading mystery picture into different shaded pictures. The created cover pictures contain less clamor contrasted with the ones already acquired utilizing the first Chang's implanting calculation. This outcomes in an extensive improvement in the sign to commotion proportion of the cover pictures by creating pictures with comparative quality to the firsts. An improvement in sign to commotion apportion of 9.3 dB and 19.97 dB were gotten for the underlying cover pictures utilized for concealing the mystery picture. This created strategy does not require any extra cryptographic calculations and accomplishes a lossless recuperation of the mystery picture. In expansion, the disguise pictures got utilizing the changed calculation look less helpless of containing a mystery message than the ones got utilizing the first strategy.

As future work, this plan can be changed to shroud two free hued mystery pictures into n important shaded spread pictures. The recuperation procedure of both mystery pictures ought to stay lossless while utilizing the same extension factor as portrayed in this paper. Secret sharing based on Lagrange interpolation is often utilized to share binary strings, but it is difficult to use for color image sharing since it yields only a limited number of shares. We therefore have developed a new color image sharing scheme based on moving lines that does not have that limitation. An implicit curve generated by moving lines is a rational curve; we believe it can therefore be directly applied for sharing compressed-domain images.

Acknowledgements

I am highly thankful to my parents, guides and friends (0139), who helped me during this research paper.

References

[1]. A. Salomaa. Public-Key cryptography. Springer, Berlin Heidelberg, 1990.
[2]. A. Shamir. How to share a secret. Communications of the ACM, 22(11):612{613, 1979
[3]. C. Blundo, A. De Bonis, and A. De Santis. Improved schemes for visual cryptography. Designs, Codes and Cryptography, 4(3):255{278, 2001.
[4]. C. Liu. Introduction to combinatorial mathematics. McGraw-Hill, New York, 1968.
[5]. C.A. Asmuth and J. Bloom. A modular approach to key safeguarding. IEEE Transactions on Information Theory, 29:208{210, 1983.
[6]. C.-C. Chang, C.-C. Lin, C.-H. Lin, and Y.-H. Chen. A novel secret image
[7]. sharing scheme in color images using small shadow images. Information Sciences, 178(11):2433{2447, 2008.
[8]. S.-K. Chen and J.-C. Lin. Fault-tolerant and progressive transmission of images. Pattern Recognition, 38(12):2466{2471, 2005.
[9]. S.-C. Chuang, C.-H. Huang, and J.-L. Wu. Unseen visible watermarking.In ICIP (3), pages 261{264, 2007.
[10]. S. Cimato, R. De Prisco, and A. De Santis. Colored visual cryptography without color darkening. Theoretical Computer Science, 374(1-3):261{ 276, 2007.
[11]. youmaran-adler-miri-qbsc2006-visual-crypto