International Journal on Emerging Technologies **3**(1): 105-108(2012)

ISSN No. (Print) : 0975-8364
ISSN No. (Online) : 2249-3255

A Review New Methodology for Visual Cryptography in Color Image Based on Cyclic Shift Pixel with Cheater Identification

Namrata Joshi*, Ankit Gupta* and Chetan Nagar*

Department of computer science & Engineering

**Jawaharlal Institute of Technology, Khargone, (M.P.)*

ABSTRACT : In this Paper a new secret visual cryptography scheme for color images based on the cyclic shifting pixels with cheater identification. Firstly, a chromatic image is decomposed into three monochromatic images using HSV color model. Secondly, these three images are transformed into binary images by using cyclic shifting pixels technique. Finally, the traditional binary secret sharing scheme is used to get the sharing images. This Scheme provides a more efficient way to hide natural images in different shares. Furthermore, the size of the shares does not vary when the number of colors appearing in the secret image differs. And also identify the cheater of shares.

Keywords: Image sharing, Visual cryptography, Image processing.

I. INTRODUCTION

Visual cryptography was originally proposed for the problem of secret sharing. Secret sharing is one of the early problems to be considered in cryptography. In a (*k*, *n*)-threshold problem, a secret is divided into n pieces. With any *k* of the *n* pieces, the secret can be perfectly reconstructed, while even complete knowledge of *k* ¡1 pieces reveals absolutely no information about the secret. Visual cryptography illustrated a new paradigm to solve the (*k*, *n*) problem. It was originally proposed by Naor and Shamir [2]. The original scheme generates n images (known as shares) based on the secret message (the original image) which can be printed on n transparencies. The original message can then be recovered if any *k* or more than *k* of the transparencies are stacked together, but no information about the original image can be gained if fewer than threshold number of k transparencies are stacked. Visual cryptography is a unique technique in the sense that the encrypted messages can be decrypted directly by the human visual system. Therefore, a system employing visual cryptography can be used by anyone without any knowledge of cryptography. Another interesting thing about visual cryptography is that it is a perfectly secure cipher. There is a simple analogy of the one time-pad cipher to visual cryptography. Besides introducing the new paradigm, Naor and Shamir also provided their constructions of visual cryptographic solutions for the general k out of n secret sharing problem. One can assume that every secret message can be represented as an image, and furthermore that the image is just a collection of black and white pixels i.e. it is assumed to be a binary image. Each original pixel appears in n modified versions (called shares) of the image, one for each transparency. Each share consists of m black and white sub-pixels. Each share of sub-pixels is printed on the transparency in close proximity (to best aid the human perception, they are typically arranged together to form a square with m selected as a square number). The resulting structure can be described by a Boolean matrix M = (mi j)n£m where mi j = 1 if and only if the j-th sub-pixel of the i-th share (transparency) is black. Usually, we will use R0 to refer to the constructed M when the pixel in the original image is white, and similarly R1 when the pixel in the original image is black. The important parameters of the scheme are: ² m, the number of pixels in a share. This parameter represents the loss in resolution from the original image to the recovered one. ² a, the relative difference in the weight between the combined shares that come from a white pixel and a black pixel in the original image. This parameter represents the loss in contrast. ² g , the size of the collection of C0 and C1. C0 refers to the sub-pixel patterns in the shares for a white pixel and black refers to the sub-pixel patterns in the shares for the 1 pixel. With the rapid development of computer and communication technology, more and more secret information are transmitted through the Internet. Therefore, the protection of the secret information from being suspected and decrypted has become critical research. In 1994, Naor and Shamir [2], invented a new information security technique, called visual cryptography scheme. It could decode the secret (handwritten notes, pictures, etc.) directly without performing any computations, and the decoder of this scheme was the human visual system. For example, in a (k, n) visual cryptography scheme, a dealer encodes a secret into n shares and gives each participant a share, where each share is a transparency. The secret will be visible if any k (or more) transparencies are stacked together; but none secret information will be revealed if the stacked transparencies are fewer than k. Such technique can be used in some areas such as conference key, private key management, multiparty computation and network auction. multimedia information is transmitted over the Internet conveniently Various confidential data such as military maps and commercial identifications are transmitted over the Internet. While using secret images, security issues should be taken into consideration because hackers may utilize weak link over communication network to steal information that they want .To deal with the security problems of secret images, various image secret sharing schemes have been developed. Visual cryptography is introduced by first in 1994 Noar and Shamir [2]. Visual cryptography is a cryptographic technique which allows visual information (e.g. printed text, handwritten notes and pictures) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. Visual cryptography scheme eliminates complex computation problem in decryption process, and the secret images can be restored by stacking operation. This property makes visual cryptography especially useful for the low computation load requirement. Overview of various visual cryptography schemes. Taking limited bandwidth and storage into consideration two criteria pixel expansion and number of shares encoded is of significance. Smaller pixel expansion results in smaller size of the share. Encoding multiple secret images into the same share images requires less overhead while sharing multiple secrets. Meaningful shares avoid attention of hacker considering the security issues over the communication channels. To meet the demand of today's multimedia information gray and color image format should be encoded by the schemes. Other performance measures such as contrast, accuracy, security and computational complexity that affect the efficiency of visual cryptography.

II. VISUAL CRYPTOGRAPHY MODEL

The model for visual cryptography is given by Naor &Shamir as follows: A printed page of cipher text and a printed transparency (which serve as a secret key). The original clear text is revealed by placing the transparency with the key over the page with the cipher, even though each one of them is indistinguishable from random noise. The model for visual secret sharing is as follows. There is a secret picture to be shared among n participants. The picture is divided into n transparencies (shares) such that if any m transparencies are placed together, the picture becomes visible. If fewer than m transparencies are placed together, nothing can be seen. Such a scheme is constructed by viewing the secret picture as a set of black and white pixels and handling each pixel separately. The most traditional visual cryptography schemes are used for black and white images.Recently, some visual cryptography schemes for gray or color images have been proposed. Verheul and Tilborg [3], present a secret sharing scheme for images with c colors. The principle of this scheme is to transform one pixel of image to b sub-pixels, and each sub pixel is divided into c color regions. In each sub-pixel, there is exactly one color region colored, and all the other color regions are black. The color of one pixel depends on the interrelations between the stacked sub-pixels. A major disadvantage of this scheme is that the number of colors and the number of sub-pixels determine the resolution of the revealed secret image. If the number of colors is large, coloring the sub-pixels will become a very difficult task. Naor and Shamir [4], propose a secret sharing scheme, which reconstructs a message with two colors by arranging the colored or transparent sub-pixels. Both approaches assign a color to a sub-pixel at a certain position, which means that displaying m colors uses m1 sub-pixels. The resulting pixels contain one colored sub-pixel and the rest of the sub-pixels are black

Therefore the more colors are used; the worse the contrast of the images becomes significantly. Their approaches cannot be applied to the extended visual cryptography either. Rijmen and Preneel [5], presented a scheme which enable multicolor with relatively less sub pixels (24 colors with m = 4). However each sheet must contain color random images, which means applying this approach to the extended visual cryptography is impossible. For this reason, Chang, Tsai and Chen recently proposed a new secret color image-sharing scheme based on the modified visual cryptography. In that scheme, through a predefined Color Index Table (CIT) and a few computations they can decode the secret image precisely. Using the concept of modified visual cryptography, the recovered secret image has the same resolution

as the original secret image in their scheme. However, the number of sub-pixels in their scheme is also in proportion to the number of colors appearing in the secret image, i.e., the more colors the secret image has, the larger the shares will become. Another disadvantage is that additional space is needed to store the Color Index Table (CIT). Extra storage capacities and special computation are required for visual data types such as images, videos or 3D objects, due to the enormity of data. Cryptographic techniques can be categorized as symmetric or asymmetric on the basis of encryption involved. Symmetric key cryptosystems are usually very fast and easy to use. Since the same key is used for Encryption and decryption, the key needs to be secure and must be shared between emitter and receiver. Asymmetric cryptosystem needs two different keys namely public and private keys. With the receiver's public key, the sender encrypts the message and sends it to the receiver who decrypts the message with his private key. Some known algorithms are RSA, El Gamal and Paillier cryptosystems. RSA and El Gamal are public-key cryptosystems which support the homomorphic operation of multiplication modulo n whereas Paillier [12] cryptosystem support homomorphic addition and subtraction of encrypted messages. Visual cryptography, a term introduced by Naor and Shamir involves the encoding of a secret image S into n shared images, where each share is distributed to a participant for security purpose but the shares do not reveal any information about the secret image and the secret image can only be revealed if the k images are stacked. The main step of RSA consists of selecting two large primes p and q, calculating their product n = p×q and selecting an integer can be addition or multiplication and not necessarily the same between the plaintexts and the ciphertexts. For two message blocks m1 (i) and m2 (i) the encryption algorithm of RSA follows the following multiplicative homomorphic property:

$$\prod_{j=1}^{l} E(m_j(i)) = E\left(\prod_{j=1}^{l} m_j(i)\right)$$

A fully-homomorphic encryption scheme E is defend by four algorithms: the standard encryption functions KeyGen E, Encrypt E, and Decrypt E, as well as a fourth function Evaluate E . Evaluate E takes in a circuit C and a tuple of cipher texts and outputs a cipher text that decrypts to the result of applying C to the plaintexts. A nontrivial scheme requires that Encrypt and Decrypt E operate in time independent of C. More precisely, the time needed to generate a cipher text for an input wire of C, or decrypt a cipher text for an output wire, is polynomial in the security parameter of the scheme (independent of C) this implies that the length of the cipher texts for the output wires is bounded by some polynomial in the security parameter (independent of C). Gentry recently proposed a scheme, based on ideal lattices, that statuses these requirements for arbitrary circuit. Complexity of KeyGen E in his initial leveled fully homomorphic encryption scheme grows linearly with the depth of C. However, under the assumption that his encryption scheme is circular secure–i.e., roughly, that it is “safe” to reveal an encryption of a secret key under its associated public key–the complexity of KeyGen E is independent of C. for more discussion on circular-security (and, more generally, key-dependent-message security) as it relates to fully homomorphic encryption. We use fully homomorphic encryption as a black box, and therefore do not discuss the details of any specie scheme. At a high-level, a derivable computation scheme is a two-party protocol in which a client chooses a function and then provides an encoding.

III. NONLINEAR METHODS

Another simple approach to image fusion is to build the fused image by the application of a simple nonlinear operator such as max or min. If in all input images the bright objects are of interest, a good choice is to compute the fused image by an pixel-by-pixel application of the maximum operator. An extension to this approach follows by the introduction of morphological operators such as opening or closing. One application is the use of conditional morphological operators by the definition of highly reliable ‘core’ features present in both images and a set of ‘potential’ features present only in one source, where the actual fusion process is performed by the application of conditional erosion and dilation operators. A further extension to this approach is image algebra, which is a high-level algebraic extension of image morphology, designed to describe all image processing operations. The basic types defined in image algebra are value sets, coordinate sets which allow the integration of different resolutions and tessellations, images and templates. For each basic type binary and unary operations are defined which reach from the basic set operations to more complex ones for the operations on images and templates. Image algebra has been used in a generic way to combine multisensor images.

IV. OPTIMIZATION APPROACHES

In this approach to image fusion, the fusion task is expressed as an Bayesian optimization problem. Using the multisensor image data and an a-prori model of the fusion result, the goal is to find the fused image which maximizes the a-posteriori probability. Due to the fact that this problem cannot be solved in general, some simplifications are introduced: All input images are modeled as markov random fields to define an energy function which describe the fusion goal. Due to the equivalence of of Gibbs random fields and markov random fields, this energy function can be expressed as a sum f so-called clique potentials, where only pixels in a predefined neighborhood affect the actual pixel. The fusion task then consists f a maximization of the energy function. Since this energy function will be non-convex in general, typically stochastic optimization procedures such as simulated annealing r modifications like iterated conditional modes will be used.

V. PROPOSED SCHEME

Images are widely used in our daily life. However, the more extensively we use the images,the more important their security will be. For example, it is important to protect diagrams of army emplacements, diagrams of bank-building construction, and the important data capturedby military satellites. In addition, the number of computer crimes has recently increased. For these reasons, image security has become an important topic in the current computer world.In this paper, we proposed a new methodology for the generation of visual cryptography. This methodology is basically a combination of Lagrange’s interpolation and Cyclic shifting cipher technique, through the Lagrange’s interpolation, We interpolate nearer distance difference of the shares generated by the users and through this equation we alsoevaluate the weight constraints factor for the pixel value shifting in X-OR operation.

On the time reconstruction of image how many minimum shared are required for thereconstruction of image. This is a challenging task for the finding or identifying a possibilityof minimum no. of shares, through this technique. We get the possibility of minimum share and also find or identify the cheaters of shares.

VI. CONCLUSIONS & FUTURE SCOPE

In this paper describes an application of presented a new kind of visual cryptography fornatural images. The new scheme provides an efficient way to share a natural image among different images. It has been shown that the size of the shares and the implementation complexity in these schemes do not depend on the number of colors appearing in the secret image. Furthermore, according to different basic matrixes, the present method can be easily extended to (k, n) threshold and arbitrary use of the visual structure for natural images processing. Visual cryptography schemes are studied and their performance is evaluated on four criteria: number of secret images, pixel expansion, image format and type of share generated. While selecting visual cryptography.

This paper the Lagrange's interpolation on cyclic shifting method consume the text use amount of calculation. So that process invites time attack in image cryptography, In future we have minimized the calculation of time and time attacks

REFERENCES

[1] Wei Qiao, Hongdong Yin, Huaqing Liang," Visual Cryptography Scheme For Color Images Based on Halftone Technique" China University of Petroleum Beijing, *IEEE* 102249, China (2009).

[2] M. Naor, and A Shamir, "Visual Cryptography," Proceeding of Euro crypt 94 Lecture Notes in Computer Science, LNCS963, Berlin: Springer, pp1-11 (1994).

[3] E. R. Verheul, and H.C.A. Tilborg, "Constructions and properties of k out of n visual secret sharing schemes," *Designs, Codes and Cryptography*, 11(2): pp 179-196, (1997).

[4] M. Naor, and A Shamir, "Visual Cryptography II: Improving the Contrast via the CoverBase," In Proc. of Security protocols. international workshop 1996, *Lecture Notes in_Computer Science* No. 1189, Springer-Verlag, pp 69-74, (1997).

[5] V. Rijmen, and B. Preneel, "Efficient Color Visual/Encryption for Shared Color of Benitton, 'Eurocryp' 96, Rump Session, Berlin, 1996, Availableathttp://www.iacr.org/conferences/ec96/rump/preneel.ps.

[6] C. Chang., C. Tsai, and T. Chen, "A new scheme for sharing secret color images in computer network," *Proceedings of International Conference on Parallel and Distributed Systems*, 2000(7), pp 21–27, (2000).

[7] Y. C. Hou, "Visual Cryptography for Color Images," Pattern Recognition, 2003, (36), pp 1619-1629, (2003).