EFFICIENT VISUAL CRYPTOGRAPHY FOR GENERAL ACCESS STRUCTURES WITH STAMPING AND SYNTHESIZING

[1]P.Lakshmi, [2]S.Baskari

ABSTRACT -- Visual cryptography is a popular solution for image encryption. The encryption procedure encrypts a image into the so-called shares which are noise-like secure images which can be transmitted or distributed over an untrusted communication channel. Using the properties of the human visual system to force the recognition of a secret message from overlapping shares, the image is decrypted without additional computations and any knowledge of cryptography. Visual cryptographic solutions operate on binary or binarized inputs. The natural (continuous-tone) images must be first converted into halftone images by using the density of the net dots to simulate the original gray or color levels in the target binary representation. Then, the halftone version of the input image is used instead of the original image to produce the shares. The decrypted image is obtained by stacking the shares together. Due to the nature of the algorithm, the decrypted image is darker, contains a number of visual impairments, and most of visual cryptography solutions increase the spatial resolution of the image. In addition, the requirement for inputs of the binary or dithered nature only limits the applicability of visual cryptography.

Keywords: General Access Structures (GAS), Pixel Expansion, Random Grids(RG) and Visual Cryptography (VC).

1 INTRODUCTION

Image processing is a method to convert an image into digital form and perform some operations on it, in order to get an enhanced image or to extract some useful information from it. It is a type of signal dispensation in which the input is an image, like video frame or photograph and output may be image or characteristics associated with that image.

- ***Lakshmi.P*** *is currently pursuing master degree program in computer science engineering. Ph-9940596145.*
- ***Baskari.S****, M.E., A.P/ CSE Dept, Ph-9710528885*

Usually image processing system includes treating images as two dimensional signals while applying already set signal processing methods to them. Image processing is any form of signal processing for which the input is an image, such as a photograph or video frame and the output of image processing may be either an image or a set of characteristics or parameters related to the image.

Most image-processing techniques involve treating the image as a two-dimensional signal and applying standard signal-processing techniques to it. Image processing usually refers to digital image processing, but optical and analog image processing also are possible. Image processing refers to processing of a 2D picture by a computer. An image defined in the "real world" is considered to be a function of two real variables, for example, a(x, y) with a as the amplitude (e.g. brightness) of the image at the real co-ordinate position (x,y). Modern digital technology has made it possible to manipulate multi-dimensional signals with systems that range from simple digital circuits to advanced parallel computers An image may be considered to contain sub-images sometimes referred to as regions-of-interest, ROIs, or simply regions.

This concept reflects the fact that images frequently contain collections of objects each of which can be the basis for a region. In a sophisticated image processing system, it is possible to apply specific image processing operations to selected regions. Thus one part of an image (region) might be processed to suppress motion blur while another part might be processed to improve color rendition. The digitized image is processed by a computer. To display a digital image, it is first converted into analog signal, which is scanned onto a display. Before processing an image, it is converted into a digital form. Digitization includes sampling of image and quantization of sampled values. After converting the image into bit information, processing is performed.

II RELATED WORK

Feng Liu State Key Lab. [1]Of Inf. Security, Chinese Acad. Of Sci., Beijing, China Chuankun Wu Xijun Lin explains construction of visual cryptography schemes in detail. The size of generated transparencies is unexpanded. Storing the shares in a safe repository. Enhancing the visual clarity of the image before processing the images. There exist other algorithms that could improve or maximize the light contrast in the reconstructed result is another topic worthy of further study. Visual cryptography provides a secure way to secure images. In this paper, the author discussed about the cheating problem in VC and extended VC. They've considered the attacks of malicious adversaries who may deviate from the scheme in any way. This paper proposes three cheating methods and applied them on attacking existent VC or extended VC schemes. Visual cryptography scheme encodes a black & white secret image into n shadow images called shares which are distributed to the n participants.

Carlo Blundo, Stelvio Cimato and Alfredo De Santis[2] explains Visual cryptography schemes with optimal pixel expansion. It classifies the image retrieval into text based and content based, including the newly growing ontology based image retrieval system as one focus. Semantic based image retrieval is an outstanding technique in retrieving the images from the image database. Since it's a survey paper, the rule base and fuzzy inference specified in the semantic based image retrieval is not clearly explained. Most of the things specified in this paper is concept based and there is no clear cut algorithm or specifications related to weight assignment operator, feature extraction and access formalities on image databases. Semantic based image retrieval is an outstanding technique in retrieving the images from the image database.

Haibo Zhang, Xiaofei Wang, Wanhua Cao and Youpeng Huang[3] explains Visual cryptography for general access structures in detail. It provides a combinational cryptography and steganography concept for strongest secure systems. Zero truncation of the pixel value is an added advantage in this project. The cipher text is retrieved by obtaining the difference in the pixel value from the closest predefined value (zero truncation). Truncation of multimedia content in this project is one of the major drawback. This paper emphasize the usage of jpeg file and it remains a major drawback if in case of using different image types. This paper didn't explain the impact of using other image types. This paper provides a basic analysis of a cheating problem in the GTCP(generic transformation for cheating prevention scheme), and present the cheating method applied it to attack on the GTCP.

Stefan Droste[4] explains New Result on Visual Cryptography in detail. The human visual system to decrypt secret images without computation the t out of n threshold Scheme and can be applied to gray-level and color images easily. Visual cryptography is that it exploits human eyes to decrypt secret images with no computation required. They've considered the attacks of malicious adversaries who may deviate from the scheme in any way. This project proposes three cheating methods and applied them on attacking existent VC or extended VC schemes. The author have proposed a systematic way of issues around the visual cryptography. Suggestions/Experimental verifications were provided towards improving the security. Overhead of the proposed technique is near optimal in both contrast degression and pixel expansion. Thus one part of an image (region) might be processed to suppress motion blur while another part might be processed to improve color rendition. The digitized image is processed by a computer. To display a digital image, it is first converted into analog signal, which is scanned onto a display. Before processing an image, it is converted into a digital form. Digitization includes sampling of image and quantization of sampled values. After converting the image into bit information, processing is performed

Yang[5] et al Visual cryptography schemes allow the encoding of a secret image, consisting of black or white pixels, into n shares which are distributed to the participants. The shares are such that only qualified subsets of participants can 'visually' recover the secret image. The secret pixels are shared with techniques that subdivide each secret pixel into a certain number m, $m \geq 2$ of subpixels. Such a parameter m is called pixel expansion. Recently Yang introduced a probabilistic model. In such a model the pixel expansion m is 1, that is, there is no pixel expansion. The reconstruction of the image however is probabilistic, meaning that a secret pixel will be correctly reconstructed only with a certain probability. In this paper we propose a generalization of the model proposed by Yang. In our model we fix the pixel expansion $m \geq 1$ that can be tolerated and we consider probabilistic schemes attaining such a pixel expansion. For $m = 1$ our model reduces to the one of Yang. For big enough values of m, for which a deterministic scheme exists, our model reduces to the classical deterministic model. We show that between these two extremes one can trade the probability factor of the scheme

with the pixel expansion. Moreover, we prove that there is a one-to-one mapping between deterministic schemes and probabilistic schemes with no pixel expansion, where contrast is traded for the probability factor without having to perform the entire protocol exchange.

2.1 PROPOSED SYSTEM

The system involves an automatic segregator of images which is a two step process of converting any images into the required Visual cryptography formatted images (Converting the mode of the image and size of the image).After getting the exact image, the images will be bifurcated into various shares depends on the access structure. In our project, we have a secret image which needs to be encoding into shares printed on transparencies. Option of providing decision of the number of shares to the user is the new feature introduced. The shares of the images appear random and contain no decipherable information's about the underlying secret image. Still,, if any 2 or more (Based on access structure) of the shares are stacked on top of one another the secret image becomes decipherable by the human eye.

Once the shares were taken the shares needs to be stamped with the help of "Stamping Algorithm". So that, a clear picture of segregating the images based on the viewable identifiers. The process involves two step process of removing the stamp and de-ciphers the logic behind the share spread and everything will be decided based on the underlying access structure.

Enhancing the clarity of the image before processing for shares and after stamping is an important feature and provides added advantage while extracting and deciphering. The shared images will be stored in the database.

The secured images can be transmitted or distributed over an un trusted communication channel. Using the properties of the human visual system to force the recognition of a secret message from overlapping shares, the image is decrypted without additional computations and any knowledge of cryptography.

III SYSTEM ARCHITECTURE

The System Architecture for Encryption and decryption process is shown in Fig.1.

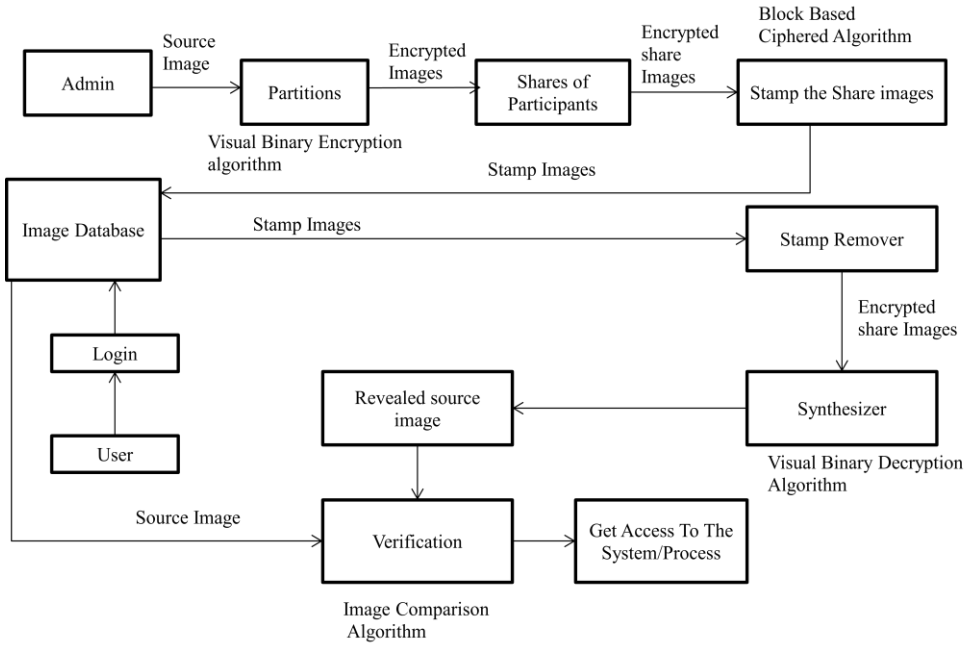

Fig .1 Encryption and Decryption Process

The visual encryption technique split the source image into more than one share images, which are encrypted images. They have only black and white pixels. The share images are stored in repository for future reference. User will give the encrypted images to the verification, where stamp remover will remove and give the encrypted images and those encrypted images are merged and revealed the original image, then verification process will check with source image of the shares from repository to validate and provide access. Such scenarios are quite common because data users often reanalyze results, conduct new analysis on intermediate data sets, or share some intermediate results with others for collaboration. Usually, intermediate data sets in cloud are accessed and processed by multiple parties, but rarely controlled by original data set holders. In the proposed system an intermediate datasets are created for a Government application where all the people related information is present. When an original dataset is being processed, the intermediate datasets are created When these intermediate datasets are collected together by an adversary it can menace the privacy-sensitive information from them, bringing considerable economic loss.

IV ALGORITHM DESCRIPTION

A. Representative Visual Encryption algorithm

The source image is converted to black and white (not grayscale, true black and white with pixels of only these two different colors). A key image is generated, of the same dimensions, where each pixel is randomly set to white or black. The original image is encrypted using this key - if the pixel in the key is white then the corresponding pixel in the original image is used in the encrypted image, whereas if the key pixel is black then the corresponding pixel in the original image is flipped (black to white, white to black) for the encrypted image.

The result is two images of apparently random black and white pixels. Each image is then doubled in size - each pixel becomes a 2x2 square of pixels. Black pixels have black pixels in the top-left and bottom-right corners while the other two pixels are while, while a white pixel in the original image produces the opposite 2x2 square. These enlarged images are the final, encrypted ones they have the appearance of random static, or snow, and neither one can be decrypted on its own no matter how powerful the computer or clever the analyst.One share is laid over the other, the original image is suddenly revealed. This is because a black pixel in the original image produced pixels of different color in the key and encrypted images (one black, one white). Since these black and white pixels became 2x2 squares with two black and two white pixels, when overlaid all four pixels in the square become black. However, a white pixel in the original produced pixels of matching color in the key and encrypted images (both black, or both white). Hence the 2x2 squares in the final images are identical, and when overlaid half the pixels remain white. Hence, when you look at the image from anything but very short range, these 2x2 squares look grey while other looks black.

B. Image Comparison and Merging Algorithm

This algorithm is similar to the classic algorithm, but accepts an amount of unexpected pixels. It splits every pixel in it's three sub-pixels red, green and blue. Afterwards it checks every actual color value against the expected color value. The final result is the amount of identical pixels divided by the total amount of pixels. The calculated result is checked against an expected value. If your images are not rendered fully deterministic but you accept a certain percentage of unexpected pixels, this algorithm may be useful are used to have shifts or distortions. . For better transformation the block size should be small, because fewer pixels keep their neighbors. In this case, the correlation will be decreased and thus it becomes difficult to predict the value of any given pixel from the values of its neighbors. At the receiver side, the original image can be obtained by the inverse transformation of the blocks.

A block cipher consists of two paired algorithms, one for encryption, E, and the other for decryption, D. Both algorithms accept two inputs: an input block of size n bits and a key of size k bits; and both yield an n-bit output block. The decryption algorithm D is defined to be the inverse function of encryption, which takes as input a key K of bit length k, called the key size, and a bit string P of length n, called the block size, and returns a string C of n bits. P is called the plaintext, and C is termed the cipher text. For each K, the function EK (P) is required to be an invertible mapping on {0,1}n. A block cipher encryption algorithm might take a 128-bit block of plaintext as input, and output a corresponding 128-bit block of cipher text. The exact transformation is controlled using a second input – the secret key. Decryption is similar the decryption algorithm takes, a 128-bit block of cipher text together with the secret key, and yields the original 128-bit block of plain text.

V EXPERIMENTAL RESULTS & SCREENSHOTS

This technique provide protection against unauthorized data access and secure dissemination of sensitive information, it can be used in authentication process in various applications like bio-metric authentication, bank and financial applications to provide more security.

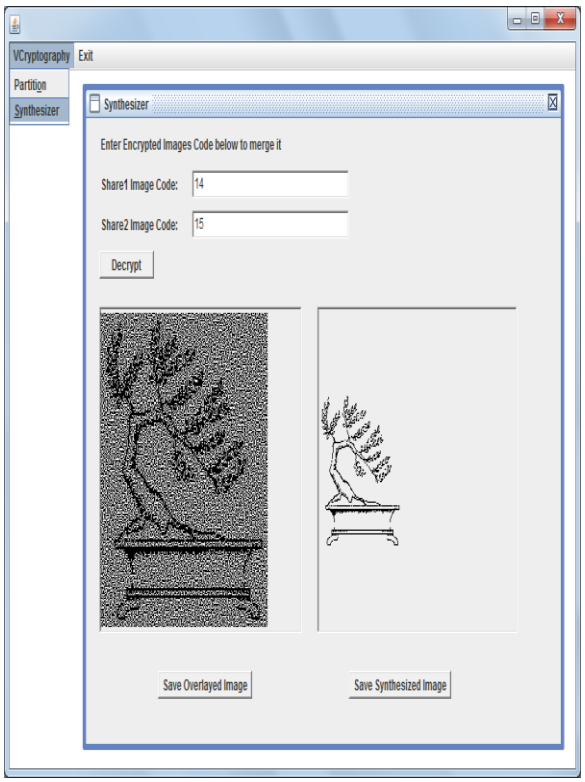

Fig .2. Synthesize the shares

VI CONCLUSION &FUTUREWORK

The system encrypts the source image and split into more than one share images and hide the original image information. Share images will have black and white pixels, are randomly moved to different share image from the source image. One image contains random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the images required to reveal the information. This technique provide protection against unauthorized data access and secure dissemination of sensitive information, it can be used in authentication process in various applications like bio-metric authentication, bank and financial applications to provide more security.

VII REFERENCES

1. Shyong Jian Shyu, "Visual Cryptograms of Random Grids for General Access Structures," Inform. Computer, vol. 23,s.no. 3, March 2013.

2. C. Blunder, S. Camano, and A. De Saints, "Visual cryptography schemes with optimal pixel expansion," Theory. Computer. Sci., vol. 369, 2006.

3. C. Blunder, P. D'Arcy, A. De Satins, and D. R. Stinson, "Contrast optimal threshold visual cryptography schemes," SIAM J. Discrete Math., 2003

4. C. Blunder, A. De Saints, and D.R. Stinson, "On the contrast in visual Cryptography schemes," J. Cryptology, vol. 12, no. 4, pp. 261–289, 1999.

[1]Lakshmi.P received degree B.E Information Technology from Periyar Maniammai College of Technology for Women,Vallam,Bharadhidasan university in 2003. Now pursuing M.E Computer Science and Engineering in Meenakshi College of Engineering, Anna university, Chennai. Ph-9940596145.

[2]Baskari.S received the B.Tech(CSE) from Dr. M.G.R. Educational and Research Institute, Chennai, in 2008 and M.Tech(CSE) from Dr. M.G.R. Educational and Research Institute, Chennai in 2011. Currently, She is an Assistant Professor in the Computer Science Department, from Meenakshi College of Engineering. ph-9715028885

