

Visual Cryptography using Invisible Watermarking of Shares

Manavi Agrawal¹ Sujata Bangar² Priyanka Padman³ Mithila Waghmare⁴

^{1,2,3,4}Department of Computer Engineering

^{1,2,3,4}Savitribai phule pune university, Bharti Vidyapeeth College of Engineering for Women, Pune

Abstract— In this project, we are taking one image and watermarking it with a secret image using DCT and IDCT algorithms. After that we are going to make 2 shares from the watermarked image. One share will be stored into database and the other share will be given to the user with ID attached to it. This is the registration phase for the user. In authentication phase, user will bring the share given to him. This share will find the share stored in database by using the ID attached. Then by superimposing these two shares we will get watermarked image generated in registration phase. Then we will apply IDCT followed by DCT on watermarked image to make secret image visible in the watermarked image and then we extract secret image from the watermark image and then we match this secret with original secret image and if matched then authenticated. The initial model developed only for the bi-level or binary images or monochrome images. Later it was advanced to suit for the colour images means gray images and RGB/CMY Images. For the RGB/CMY Images different methods are developed based on the colour decomposition techniques. Visual cryptography scheme is the concept of encrypting a secret image into n (more than one) shares. Rotation Visual Cryptography scheme (RVCS) allows four secret images to be encrypted into two shares. Using Human Visual System, again the four secret images can be easily recovered by placing the two shares on top of each other with different angles. In this paper proposes a Rotation Visual Cryptography using basic (2,2) scheme which encrypts three secret images into three shares and each secret image can be easily revealed by overlaying one share with the 1800 anticlockwise rotation of another share. In this way the combination of any of the two shares reveals one secret image with the help of 1800 anticlockwise rotation. The reconstructed original three secret images have the same contrast as achieved in the basic visual cryptography scheme (2, 2).

Key words: Watermarking, Secret Image, DCT, IDCT

I. INTRODUCTION

A. Aim:

To perform Visual Cryptography on images which is used to secure the images. In visual cryptography the image is divided into parts called shares and then they are distributed to the participants.

B. Motivation:

The field of encryption is becoming very important in the present era. Security is an important issue in communication and storage of images, and encryption is one of the ways to ensure security. Image encryption has applications in internet communication, multimedia systems, medical imaging, telemedicine, military communication, etc. Images are different from text. Although we may use the traditional cryptosystems to encrypt images directly, it is not a good idea for two reasons. One is that the image size is almost always much greater than that of text. Therefore, the

traditional cryptosystems need much time to directly encrypt the image data. The other problem is that the decrypted text must be equal to the original text. However, this requirement is not necessary for image data. Due to the characteristic of human perception, a decrypted image containing small distortion is usually acceptable.

Visual cryptography was pioneered by Moni Naor and Adi Shamir in 1994. They demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any $n-1$ shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear. Visual cryptography is a new technique which provides information security which uses simple algorithm unlike the complex, computationally intensive algorithms used in other techniques like traditional cryptography. This technique allows Visual information (pictures, text, etc) to be encrypted in such a way that their decryption can be performed by the human visual system, without any complex cryptographic algorithms.

This technique is called as (k, n) VCS model where k represents the minimum no. of shares needed to decrypt the secret image (image which is to be secured) and n represents the no of shares generated by the scheme. Digital watermarking is the act of hiding a message related to a digital signal (i.e. an image, song, and video) within the signal itself. It is a concept closely related to steganography, in that they both hide a message inside a digital signal. However, what separates them is their goal. Watermarking tries to hide a message related to the actual content of the digital signal, while in steganography the digital signal has no relation to the message, and it is merely used as a cover to hide its existence.

Watermarking has been around for several centuries, in the form of watermarks found initially in plain paper and subsequently in paper bills. However, the field of digital watermarking was only developed during the last 15 years and it is now being used for many different applications.

II. RELATED WORK

Visual cryptography was pioneered by Moni Naor and Adi Shamir in 1994. They demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any $n-1$ shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear. Visual cryptography is a new technique which provides information security which uses simple algorithm unlike the complex, computationally intensive algorithms used in other techniques like traditional cryptography. This technique allows Visual information

(pictures, text, etc) to be encrypted in such a way that their decryption can be performed by the human visual system, without any complex cryptographic algorithms.

This technique is called as (k, n) VCS model where k represents the minimum no. of shares needed to decrypt the secret image (image which is to be secured) and n represents the no of shares generated by the scheme.

Digital watermarking is the act of hiding a message related to a digital signal (i.e. an image, song, video) within the signal itself. It is a concept closely related to steganography, in that they both hide a message inside a digital signal. However, what separates them is their goal. Watermarking tries to hide a message related to the actual content of the digital signal, while in steganography the digital signal has no relation to the message, and it is merely used as a cover to hide its existence.

Watermarking has been around for several centuries, in the form of watermarks found initially in plain paper and subsequently in paper bills. However, the field of digital watermarking was only developed during the last 15 years and it is now being used for many different applications.

III. ARCHITECTURE DIAGRAM

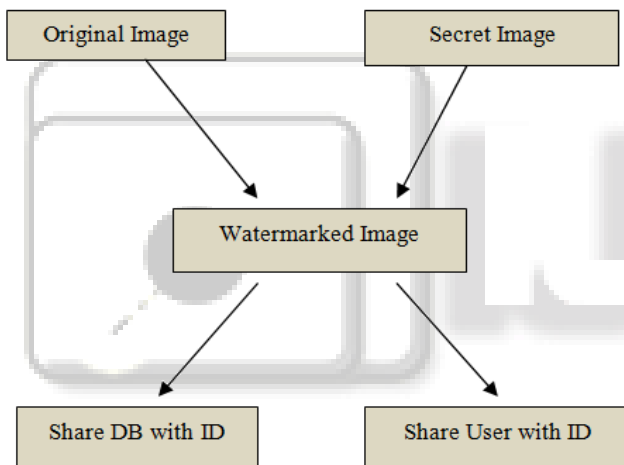
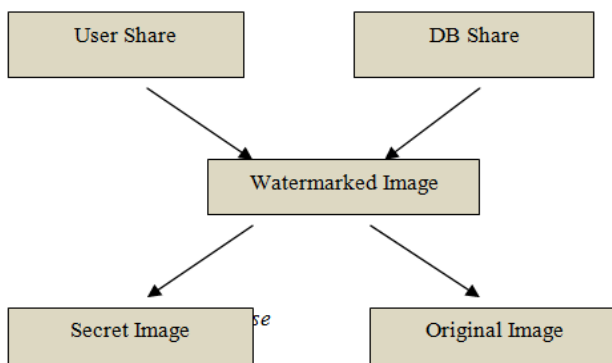


Fig. 1: Registration Phase



IV. WORKING

A. Registration Phase:

1) Original Image:

Original Image is the user's images taken while registration.

2) Secret Image:

Secret Image is the image we are going to use for watermarking

3) Watermarked Image:

We are applying DCT on Original and Secret Image to get watermarked Image

4) Share DB with ID:

We are storing a share into database

5) Share User with ID:

We are giving one share to the user with an ID.

In this project, we are taking one image and watermarking it with a secret image using DCT and IDCT algorithms. After that we are going to make 2 shares from the watermarked image. One share will be stored into database and the other share will be given to the user with ID attached to it. This is the registration phase for the user.

B. Authentication Phase:

1) Share DB with ID:

We are storing a share into database

2) Share User with ID:

We are giving one share to the user with an ID.

3) Watermarked Image:

By superimposing both the shares we will get watermarked Image.

4) Secret Image:

It is the image we are getting by using IDCT algorithm on watermarked image.

5) Original Image:

By applying IDCT on watermarked image it will separate secret image and original image, which we can compare to authenticate the user

In authentication phase, user will bring the share given to him. This share will find the share stored in database by using the ID attached.

Then by superimposing these two shares we will get watermarked image generated in registration phase. Then we will apply IDCT followed by DCT on watermarked image to make secret image visible in the watermarked image and then we extract secret image from the watermark image and then we match this secret with original secret image and if matched then authenticated.

V. ALGORITHMS

A. DCT:

A discrete cosine transform (DCT) expresses a finite sequence of data points in terms of a sum of cosine function oscillating at different frequencies. DCTs are important to numerous applications in science and engineering, from lossy compression of audio (e.g. MP3) and images (e.g. JPEG) (where small high-frequency components can be discarded), to spectral methods for the numerical solution of partial differential equations. The use of cosine rather than sine functions is critical for compression, since it turns out (as described below) that fewer cosine functions are needed to approximate a typical signal, whereas for differential equations the cosines express a particular choice of boundary conditions.

In particular, a DCT is a Fourier-related transform similar to the discrete Fourier transform (DFT), but using only real numbers. DCTs are equivalent to DFTs of roughly twice the length, operating on real data with even symmetry (since the Fourier transform of a real and even function is real and even), where in some variants the input and/or

output data are shifted by half a sample. There are eight standard DCT variants, of which four are common.

The most common variant of discrete cosine transform is the type-II DCT, which is often called simply "the DCT", [1][2] its inverse, the type-III DCT, is correspondingly often called simply "the inverse DCT" or "the IDCT". Two related transforms are the discrete sine transform (DST), which is equivalent to a DFT of real and odd functions, and the modified discrete cosine transform (MDCT), which is based on a DCT of overlapping data.

B. IDCT:

$$X_k = \frac{1}{2}x_0 + \sum_{n=1}^{N-1} x_n \cos \left[\frac{\pi}{N} n \left(k + \frac{1}{2} \right) \right] \quad k = 0, \dots, N-1.$$

Because it is the inverse of DCT-II (up to a scale factor, see below), this form is sometimes simply referred to as "the inverse DCT" ("IDCT"). [2]

Some authors further divide the x_0 term by $\sqrt{2}$ (resulting in an overall $x_0/\sqrt{2}$ term) and multiply the resulting matrix by an overall scale factor of $\sqrt{2/N}$ (see above for the corresponding change in DCT-II), so that the DCT-II and DCT-III are transposes of one another. This makes the DCT-III matrix original, but breaks the direct correspondence with a real-even DFT of half-shifted output. The DCT-III implies the boundary conditions: x_n is even around $n=0$ and odd around $n=N$; X_k is even around $k = -1/2$ and even around $k=N-1/2$.

VI. ACTIVITY DIAGRAM

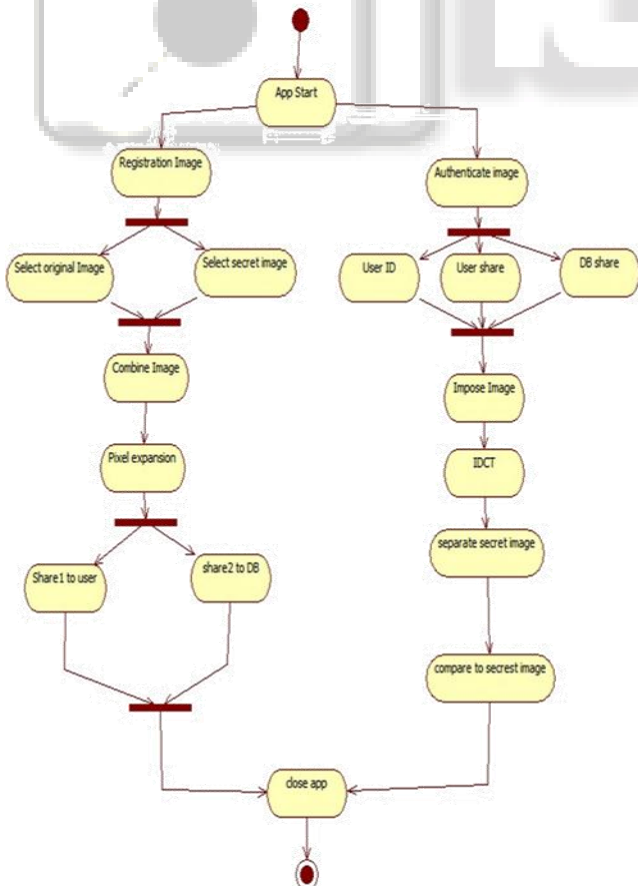


Fig. 2: Activity Diagram

VII. RESULT OF OUR SYSTEM

The proposed scheme achieves effective embedding of the binary share images into the host images. Also, the proposed scheme depicts efficient extraction of the embedded watermarks from the watermarked images. The watermarked images possess good Peak Signal to Noise Ratio (PSNR) and good visual quality. Fig. 5 depicts the results obtained on experimentation of the entire proposed Visual Cryptography scheme. The results include original secret image, encoded secret shares, host image, watermarked images and the decoded secret image.

VIII. ADVANTAGE

A. Cheaper Solution Than Smart Cards, Hardware Tokens, Software Tokens & USB Tokens:

Smart cards, hardware tokens are the hardware tools used for authenticating the users which comes with a cost. But in our application we are using PC's camera to take an image and then our written algorithm will decide whether user is valid or invalid. So it saves the cost of hardware tools for each user.

B. Password Is Split Into Shares, So Hacking The Server Will Not Result Into Anything:

In traditional approach, passwords are stored on the central server. Hackers can hack the server by using methods such as SQL Injection, Brute Force Methods. If the centralized server gets hacked then all the critical data will be available to hacker. So in our application we are storing only half data on server which is meaningless until hacker get the another half part which is with the user.

C. Watermark Added An Extra Security:

In normal cryptographic solutions, the shares are not authenticated. So user may bring in the invalid share which may cause the system to go down. In our case, we are adding an extra security by using DCT algorithm which will watermark the shares so that double authentication is provided.

IX. DISADVANTAGES

A. Processing Time Increased Due To Watermark Addition:

In cryptographic and watermarking algorithms we are not dealing with the text passwords. Here we are dealing with images which bring in the Image processing algorithm execution. There are many complex processes are done on a single image such as Binarization, Feature Extraction etc. Which increase the time complexity of the system to an greater extent than normal text processing.

X. APPLICATIONS

A. Protection of Visual Cryptography:

The watermark method is an excellent technique to protect the copyright ownership of a digital image.

The proposed watermark method is built up on the concept of visual cryptography. According to the proposed method, the watermark pattern does not have to be embedded into the original image directly, which makes it harder to detect or recover from the marked image in an

illegal way. It can be retrieved from the marked image without making comparison with the original image.

B. Prevention from Unauthorized Copying:

Digital watermarking technique is one of the solutions to avoid unauthorized copying or tampering of multimedia data. Recently many watermarking schemes have been proposed to address this problem. The watermarking schemes are broadly categories into two main domains i.e. spatial domain and the transform domain.

C. Authentication:

Biometrics deal with automated methods of identifying a person or verifying the identity of a person based on physiological or behavioral characteristics. Visual cryptography is a secret sharing scheme where a secret image is encrypted into the shares which independently disclose no information about the original secret image. As biometric template are stored in the centralized database, due to security threats biometric template may be modified by attacker. If biometric template is altered authorized user will not be allowed to access the resource. To deal this issue visual cryptography schemes can be applied to secure the iris template. Visual cryptography provides great means for helping such security needs as well as extra layer of authentication.

D. Can Be Used In High Security Zones:

The implementation of this application is feasible for high security zones only because the process of registration and Authentication is time consuming. If we try to use this system for crowdie places then it is not feasible to manage the flow of users coming in and going out.

XI. ACKNOWLEDGMENT

We take this great opportunity to thank everyone who has contributed to our Project in some or the other way.

We would firstly like to thank to H.O.D. of our Computer Department Prof. D. D. Pukale for letting us this great opportunity to test our skill through creation of our project as a part of our syllabus.

Special thanks must goes to Prof. Mrs. V. D. Kulkarni for her guidance for developing this project.

REFERENCES

- [1] Ateniese.G, Blundo.C, De. Santis.A, and Stinson.D.R, "Visual cryptography for general access structures," *Inf. Computat.*, vol. 129, pp. 86–106, 1996.
- [2] Ateniese.G, Blundo.C, De. Santis.A, and Stinson.D.R, "Constructions and bounds for visual Cryptography," *Lecture Notes Computer Sci.*, vol. 1099, pp. 416–428, 1996.
- [3] Blakley.G.R, "Safeguarding cryptographic keys," in *Proc. Nat. Computer Conf.*, 1979, vol. 48, pp. 313–317.
- [4] Blundo.C, De. Santis.A, and Stinson.D.R, "On the contrast in visual cryptography," *J. Cryptology*, vol. 12, pp. 261–289, 1999.
- [5] Blundo.C, D'Arco.P, De. Santis.A, and Stinson.D.R, "Contrast optimal threshold visual

Cryptography schemes," *SIAM J. Discrete Math.*, vol. 16, pp. 224–261, 2003

- [6] Blundo.C, Cimato.S, and De Santis.A, "Visual cryptography schemes with optimal pixel expansion," *Theoretical Computer Sci.*, vol. 369, pp. 169–182, 2006.