ISSN 2395-1621

Visual Cryptography with Invisible Watermarking of Shares

[#1]Sameer Machale, [#2]Aishwarya Chavan, [#3]Ravina Pihal, [#4]Amit Gaikwad, [#5]Prof. Roma Kudale

[1]sameermachale@gmail.com
[2]aschavan503@gmail.com
[3]ravina.pihal@gmail.com
[4]gaikwadamit1994@gmail.com
[5]roma.kudale@gmail.com

ABSTRACT

Visual Cryptography (VC) is a method of decoding a secret data (image, text, etc.) by human vision without any need of computation .In this paper VC technique is used with digital invisible watermarking on shares .The secret data can only be revealed when one share is superimposed with another share, out of these two shares one share is available with user and other share is present in the database. In this paper we have also proposed a new approach i.e. One Time Password (OTP) which will allow a password only for limited span of time for a particular user, thus ensuring added security .Hence in this way it will provide 3-way security from client and server side, so as to share data securely on network.

Keywords— Visual Cryptography, Watermarking, Shares, Superimposing.

ARTICLE INFO

Article History

Received :8th March 2016

Received in revised form :

10th March 2016

Accepted : 12th March 2016

Published online :

15th March 2016

I. INTRODUCTION

Visual Cryptography (VC) is an unique technique for securing the data. Visual Cryptography is an encryption method, which involves hiding of images in such a way that it can only be decrypted by human vision if correct key is used. We are using the concept called "DIGITAL WATERMARKING" in our paper.Invisible digital watermarking is used in our project. Watermarking is one way of embedding the secret image into cover image without affecting its original quality of image so that the secret image can be fetched by some process. A binary image is split into two shares which are present in the form of 0 and 1. Then one of the shares is stored in database and other is held with owner.The data is permanently stored in the database after any decryption process .The decryption process is done by overlapping these two shares i.e the image from the database and the image from the owner .If these overlapped images match then the user is authenticated and he/she can access on cloud. We also provide One-Time-Password (OTP) to our system which is an add security. So in this way we provide three way security on cloud. In a VC scheme, shares are generated from the original image according to rules of the scheme in such a way as to provide no information about the encrypted image individually, but to produce a reasonable depiction of the original image when superimposed. While the original image should be visible after overlaying its shares, visual cryptography schemes are typically lossy and produce decrypted images that are often noisy or suffer from diminished contrast and resolution. A number of factors can affect the quality of the resulting decrypted image in a VC scheme. Typically, as the number of shares n is increased, the contrast of the resulting decrypted image worsens. Furthermore, many schemes produce shares in which each pixel of the original image is represented by multiple pixels in each share, diminishing the resolution of the decrypted image. This paper presents algorithms that both do and do not require pixel expansion to highlight the differences between the two.

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, and video) within the signal itself. [12]

III.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, 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.

IV. DIFFERENT PHASES AND SYSTEM ARCHITECTURE

There are two main phases in our project Registration Phase and Authentication Phase which are shown in this

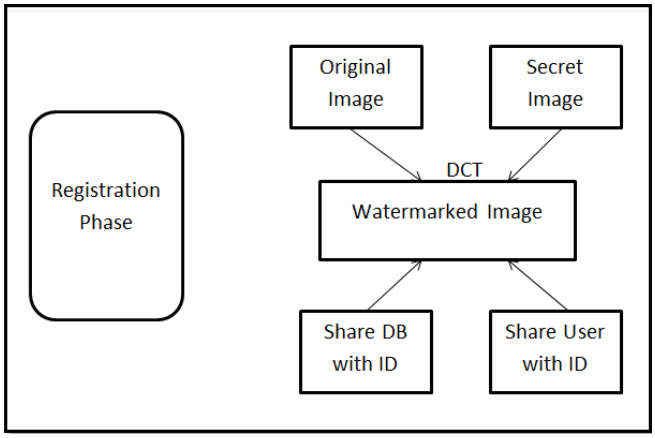

Fig 1 : Registration Phase

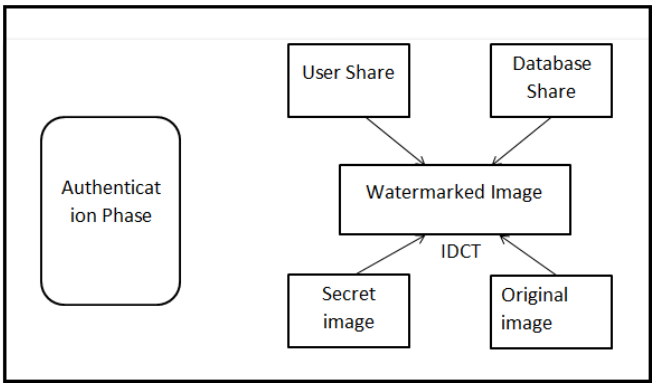

Fig 2: Authentication Phase

Our project consists of two phases as shown in (Fig 1, Fig 2) i.e. Registration phase and Authentication phase. In registration phase the user has to sign up on the cloud so that the data is stored and does not require to register again while accessing the data. In authentication phase the password generated by the user is cross-checked.

Registration Phase as shown in (Fig 1):-

In this phase the original image and secret image is watermarked using DCT algorithm. This watermarked image gets split into two share. These shares are allotted with some unique ids. Out of these two shares one share is with database and the other share is with the user along with their ids.

Authentication Phase (Fig 2):-

In this phase the shares from database and share from user are overlapped for authentication. This overlapped image generates a watermark image. Inverse discrete cosine transform (IDCT) algorithm is applied on this watermark image to get the original image and the secret image.

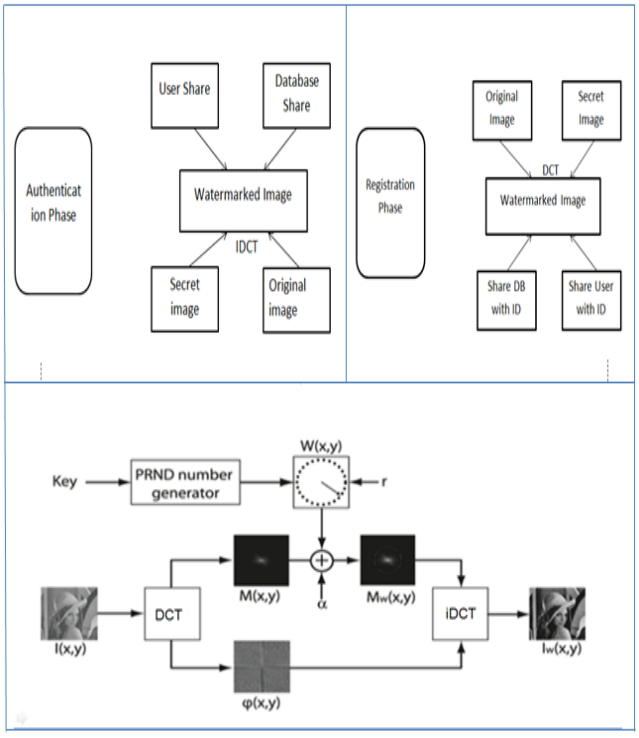

Fig 3: Proposed Architecture

V. CONCLUSION

In this project we are going to hide the information by combining the features of both steganography and visual cryptography. The proposed system is used to overcome the difficulties faced in existing system and it has several advantages like 3 levels of security, requires computation time for single level of hiding and the proposed system can be used in applications like payment gateways, military, navy, business settlement contracts Providing security to the confidential data shared in day to day life is an important issue in real life. Visual cryptographic scheme, which can decrypt secrete images without any cryptographic computations. The proposed scheme is perfectly secure and very easy to implement with low computation cost. In our proposed scheme, first the secret image is taken and then it is divided into shares after converting it into binary image, then the shares of binary image are encrypted and decrypted using RSA algorithm, because of this even if the third party or intruder, once getting all the shares, he/she can't get back the original secret image without availability of the private key. We can notice that there are many possible extensions exist as the visual quality & size of retrieved image. We can use following as some of the future extensions. 1. We can use colour image in place of binary image and then generate the shares using Visual Cryptography method. 2. Encrypted shares can compressed in order to reduce the bandwidth requirement.

ACKNOWLEDGEMENT

We take this great opportunity to thank everyone who has contributed to our project in some or other way.We would like to thank our project guide Prof. Roma Kudale and Prof.Shyam Kosbatwar for their guidance for developing this project.

REFRENCES

[1]Jagdeep Verma, Dr.Vineeta Khemchandani
"A Visual Cryptographic Technique to Secure Image Shares",International Journal of Engineering Research and Applications (IJERA) 'ISSN: 2248-9622'.
[2] Malvika Gupta, Rajan Verma
"Digital Watermarking to Secure Image Shares: A Visual Cryptographic Scheme", International Journal of Latest Trends in Engineering and Technology (IJLTET).
[3] Shyamalendu Kandar, Arnab Maiti, Bibhas Chandra Dhara
"Visual Cryptography Scheme for Color Image Using Random Number with Enveloping by Digital Watermarking", International Journal of Computer Science I ssues (ISSN: 1694-0814).
[4] A.Umaamaheshvari, K.Thanushkodi
"A Novel Watermarking Technique Based on Visual Cryptography", International Journal of Advanced Research in Computer Engineering & Technology.
[5] Malvika Gupta, Deepti Chauhan
"A Visual Cryptographic Scheme To Secure Image Shares Using Digital Watermarking"International Journal of Computer Science and Information Technologies (IJCSIT).
[6] Amir Houmansadr*, Shahrokh Ghaemmaghami
"A Digital Image Watermarking Scheme Based on Visual Cryptography".
[7] Ching-Sheng Hsu and Shu-Fen Tu
"Digital Watermarking Scheme with Visual Cryptography", International MultiConference of Engineers and Computer Scientists, (IMECS 2008).
[8] Ren-Junn Hwang "A Digital Image Copyright Protection Scheme Based on Visual Cryptography", Tamkang Journal of Science and Engineering, Vol. 3.
[9] Keshav S Rawat, Dheerendra S Tomar,
"Digital watermarking schemes for Authorization against Copying or Privacy of Colour Images", Indian Journal of Computer Science and Engineering Vol. 1.
[10] Ms. Bhawna Shrivas, Prof.Shweta Yadav
"A Survey on Visual Cryptography Techniques and their Applications", International Journal of Computer Science and Information Technologies, Vol. 6 (2).
[11] Dr. Ajit, Preeti Kalra, Sonia Dhull
"International Journal of Advanced Research in Computer Science and Software Engineering",IJARCSSE.
[12] Manavi Agrawal, Sujata Bangar, Priyanka Padman, Mithila Waghmare
"Visual Cryptography using Invisible Watermarking of Share" IJSRD - International Journal for Scientific Research & Development, Vol. 3.

