Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 01, January -2018

Online Payment Security Using Image Cryptography

Lalit Manwani, Adarsh Dabhane, Anuja Sande, Reshma Sonar*

Department of Information Technology, Sinhgad College of Engineering, Pune

Abstract —*In the 21st Century, the digital payment is increasing day by day and the traditional methods of digital payment are losing its authenticity. Due to recent intrusions and attacks on the payment system making it vulnerable, whether the old systems are still robust is debatable. This paper presents a novel method of digital payment using image cryptography and watermarking techniques. The proposed system ensures a more robust and simple system for electronic payments. To achieve this, the system uses a binary image, called watermark, is split into two shares via a 2-out-of-2 visual secret sharing scheme. Then, one of the share is embedded into the host image, and the other is held by the owner. When proving the ownership, the owner has to extract the embedded share and recover the watermark with his/her own share. Based on the security property of visual cryptography, the proposed system can make sure that the two shares cannot leak any information about the watermark. Proposed Online Payment system is a software based and is universally compatible with all systems.*

Keywords- *Digital Payment, Image Cryptography, Watermarking, Visual Secret Sharing Scheme, Encryption*

I. INTRODUCTION

Online Payment systems are increasing rapidly all over the globe and the requirements for secured systems are growing than ever before. Digital Payments are expected to grow at rapid percentage year on year making a need for robust payment system. The system proposed will be helpful in delivering those necessities as well as tackling vulnerabilities of the traditional systems.

1.1 Problem Definition

In this system the aim is to provide the image based authentication that can-do login. Password image is generated and it will be downloaded from the email which is stored at the time of registration. Every time the image will be unique. The OTP based authentication is also used as per the guidelines of Reserve Bank of India.

1.2 Objectives

In this project, the aim is to provide an efficient technique to optimize to develop system that data will be embedded into the image file and video files and the system splits the image into two similar parts and send the images to the user and to the database sender sends this file to the receiver and the receiver matches the half image with the image which is with the database. Thus, developing a web application for online payment security which will let the users to make payments easily and speedily with high end encryption.

Our main objective here is to provide optimum security using the techniques described in our project to applications and organization viz. Banks, Transaction portals. With the advancements in technology, our project involves methods that are used for embedding and extracting data from the digital data.

1.3 Scope of Paper Work

The proposed system helps us to reduce the data theft and information pilfering of sensitive information. The system helps build faster communication between the user and data inserting system. The aim of the system is to have a redundant system that is able to easily and efficiently transfer data through and from the existing secured channels for any payment or transferring operation that is done. This system provides a faster and more secure way of enabling the user to ensure that the task is done with minimum hassle and easiness.

1.4 Organization of Paper

Chapter I gives a general awareness of Online Payment Using Image Cryptography, Problem Definition, its Motivation, Objectives and Scope of paper work. Chapter II describes the survey of existing Image Cryptographic

methods. Chapter III presents overview of proposed work i.e. flowcharts, experimental parameter and expected outcome of proposed work. Chapter IV shows implementation results of proposed method and Finally, Chapter V presents conclusion of overall proposed system.

II. LITERATURE SURVEY

Images can be encrypted in several ways, by using different techniques and different encryption methods. In this paper by using Huffman Coding method for image steganography, Elliptic Curve Cryptography for image encryption and Discrete Wavelet Transform for image compression. With the use of steganography, encryption and compression all together on the image data. After applying all these techniques on image data, it results in an encryption method which is highly secure [10] [11].

Cryptography is defined as the method to conceal information by encrypting plaintexts to cipher texts and later transmitting it to the intended recipient using an unknown key, on the other hand Steganography provides or say extends security further to a high level by hiding the cipher text into text, image or other formats. Steganography with the Greek word “Stegos + grafia” literally means, "covered + writing” [12].

Rupali Jain [4] describes the theory of steganography and the various implementations of steganography used in the internet. Steganographic system is generally made up of mainly cover object, secret message, stego-key, stego-system encoder, stego object and stego-system decoder. Generally, innocent looking carriers, e.g., pictures, audio, video, text, etc. that hold the hidden information is called as Cover object. On the other hand, Stego key is an additional piece of information, such as a password or mathematical variable, required to embed the secret information [4].

The process of applying stego key in order to hide secret message inside the cover object is called as stego system encoder. The combination of hidden data plus cover object is known as the stego object. Stego system decoder is the process of applying the same stego key over the stego object in order to separate the hidden message from the cover object [4].

The techniques used in image steganography is spatial domain techniques like Least Significant Bit (LSB) technique, PVD technique, Edge based technique etc. Another way of achieving it is, using transform domain techniques like DCT, DWT, DFT, IWT and DCVT.

Sadaf Bhukari [1] introduced a technique for transferring images in open channel networks channels with protection. This method depends on steganography and cryptography (double random phase encoding). The information that is to be concealed is called original image and the image in which the top-secret information (original image) is to hide is called the cover image and after that method the image obtained is a stego image. After hiding method no differentiation is found in the cover picture and the stego picture. Double random phase enciphering done on the stego image to add more randomness in the stego image and made it more secure for transmission [1]. Decrypting the whole technique is opposite of the encryption technique used. Then by applying the reverse steganography technique on decrypted image we extract the original image and also the information.

Social media is a growing internet phenomenon and is growing day by day with more people coming on the internet; therefore, protecting them against piracy is worthy of consideration. Morteza Heidari [2] proposed a watermarking method in Discrete Cosine Transform (DCT) domain. For this purpose, DCT coefficients of the whole image are calculated and then singular values of watermark image are extracted, and in an empirical way a vector of strength factors (α) is extracted for embedding. By using these strength factors, singular values of watermark image are embedded with a four-time redundancy to the low frequency DCT components located on the main diagonal of DCT matrix of the host image [2]. Finally, in the extraction side, we use the embedding redundancy, extract all four different versions of watermark and by taking advantage of voting method on them, the final watermark image is reconstructed.

Watermarking a technique which uses pattern bits are inserted in a digital image, video or audio files to have copyright information, sensitive data etc. Arisudan Tiwari [3] uses a technique in which the digital watermark is achieved using Discrete Wavelet Transform (DWT). In this technique the author uses DWT and CT to develop a blind image watermarking algorithm to provide better imperceptibility and higher robustness against variety of attacks.

The main reason of combing DWT and CT is to minimize the drawbacks of each of them separately. Most researchers in the field of digital watermarking focuses on using DWT, due to its excellent spatial localization and multi-resolution properties [3].

Ravi K Sheth [6], suggested a new secured digital watermarking technique that can be used for the data validation. The secured digital watermark is added by the hybrid method for which, the author has used combination of discrete cosine transform (DCT) and discrete wavelet transform (DWT) [6]. In this technique, the author has used DCT-DWT

based secured method to implement watermarking process. In this method along with DCT and DWT additional Arnold Transform is also used to encrypt watermark data.

Palak Patel [5], observed the effect of embedding the image (logo image) into secret image using DCT based steganography and then this watermarked image is embedded into cover image using SVD and DWT based digital watermarking for provide security as well as authenticity. The PSNR has been used to measure quality of stego image. In their proposed technique, the author has presented a combined strategy of Steganography, Digital Watermarking and Cryptography using Discrete cosine transform(DCT), Discrete wavelet transform (DWT), Singular value decomposition(SVD) and RSA algorithm which provide security of the images and as well as authenticity of the image author in the internet environment [5].

A single confidential data having multiple owners has equal authority over the data. To provide equal authority to each owner a technique known as Visual Cryptography can be used to generate N shares of secret image with each owner having one or more shares. By superimposing all shares together, original image is retrieved. Shares less than N cannot reveal the original secret image.

Vaibhav P. Sapkal [7], proposed a security for the confidential image having multiple owners. The main objective of our paper is to provide equal digital rights to the owners of the confidential image. Visual cryptography technique is used which generates N shares according to the number of owners and watermarking is used to authenticate each share with its owner. The security of the confidential data is maintained using both visual cryptography and watermarking. Thus, the proposed scheme fulfils the requirement of security and digital rights management [8].

OPT is a password that is valid for only one login session or transaction. This OPT allow the user to get login into the system by entering their password with OTP. In our proposed approach is, after user entering the username and password web server generates the Encrypted OTP using AES algorithm and send it to the users mobile. OTP is an encrypted format, so users can't read it. Instead of that, user needs to forward that OTP with system logging password to the system. At the system end encrypted OTP is decrypted and verify the OTP, Password and mobile number for a particular username.in this approach user's information is verified in many levels. It avoids the unauthorized logging [8][9].

III. PROPOSED WORK

The Proposed System will be developed using NetBeans IDE [13] and will use plugins for the mobile connecting as well as email connecting services. The software currently developed is only available for personal computers. Once the proposed system is started, the user gets an account handling screen. In the account handling screen the user can choose between creating a new account or logging in into the account

Fig 1. Sign Up Page

As shown in Fig 1, a new user is created, in which the user has to enter his credentials like email ID, address and contact information. The next thing user submits is his own image or image randomly generated by the software. This image is the main credential of the user and the software uses watermarking and steganography techniques on this image. Once the image is registered all the above techniques are carried out on the image. The proposed system then sends the user to an authentication phases of screens, in the first phase, the user enters his desired email address for the password to be sent. In the second phase, the user uploads the password given to the user by the system. And in the third phase, the user gets an OTP on the registered mobile number

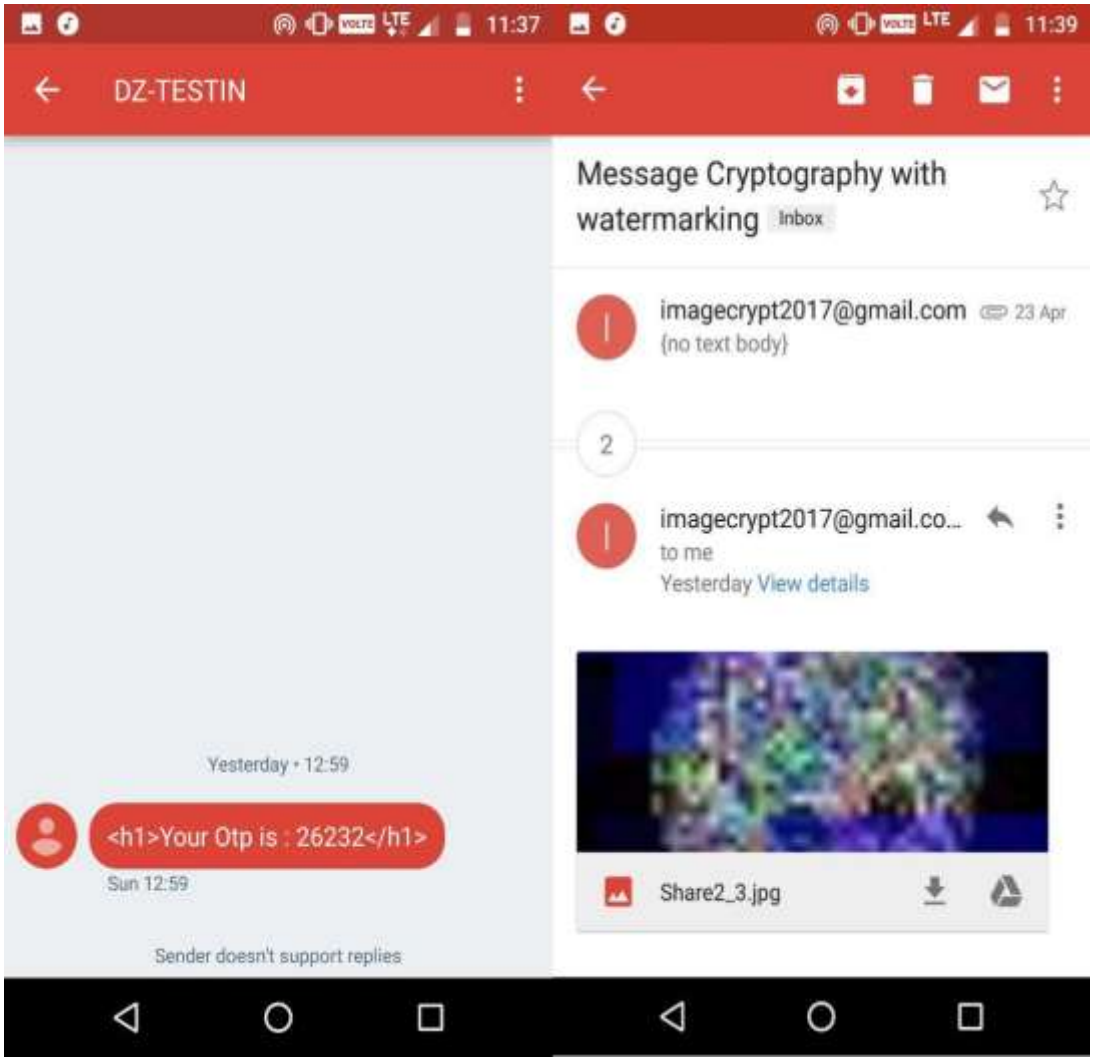

Fig 2. OTP on Mobile & Image Share

Fig 2, shows the OTP [8] received on the smartphone and also the password generated by the proposed system. The User uploads the generated password in the system and also enters the OTP sent on the mobile number given. After entering the information, the proposed system accepts the user account and loges the user into the system. The proposed system gives the user options of Logging Out, Transaction, Report. The Transaction tab then can be used by the user to do online payments more securely and more robustly. Report section tab is used for reporting any anomalies or any fault in the proposed system.

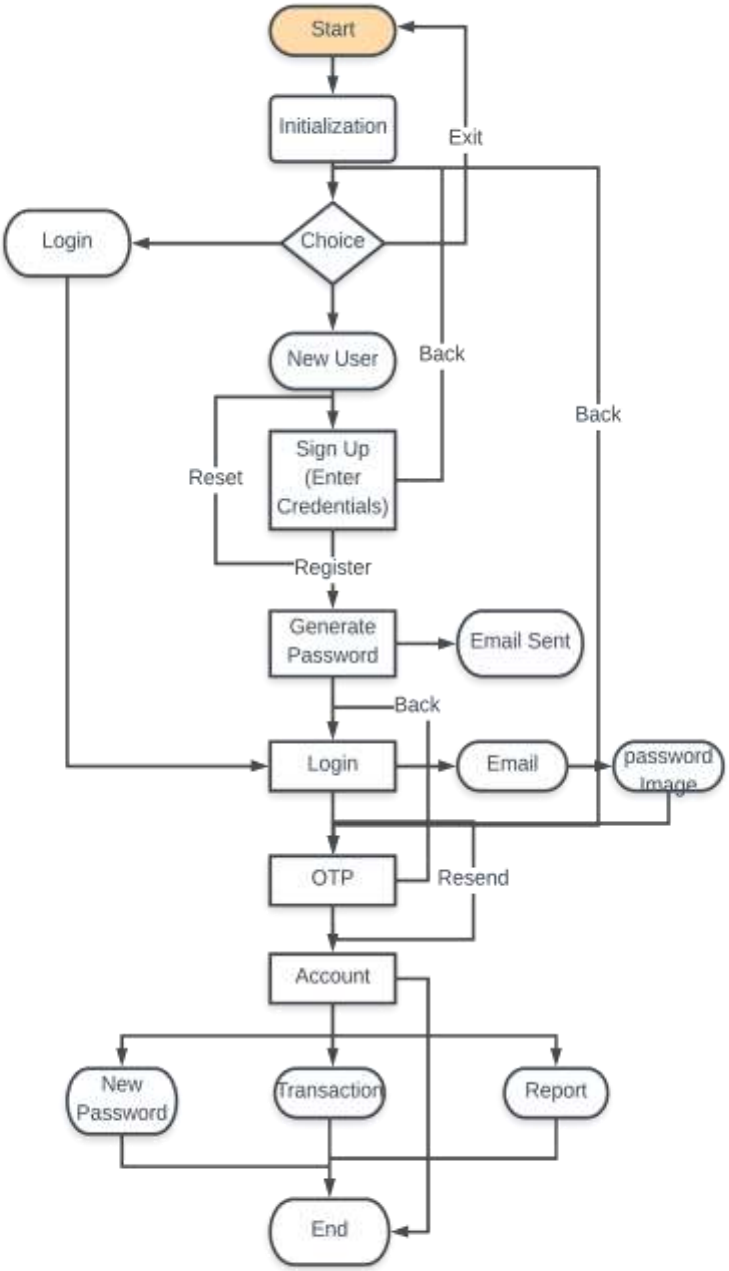

Fig 3 Flowchart of Proposed System

Fig 3 shows us the flow of the proposed system, user initializes the system and enters the credential information and proceeds further. As expected, the proposed system works as per the standards of payment systems and gives a more secured and authentic way for payments. The system enables users to have a hassle-free payment solution and give assurance of the proposed system encrypting techniques

IV. RESULTS AND EVALUATION

The proposed system is universally acceptable and meets the guidelines of the universal banking laws, and present a novel solution to the online payment system. The performance of the proposed system has been tested in different situations and the system proves to be robust. The system has also been analyzed for prevention of different attacks like phishing, injection methods etc.

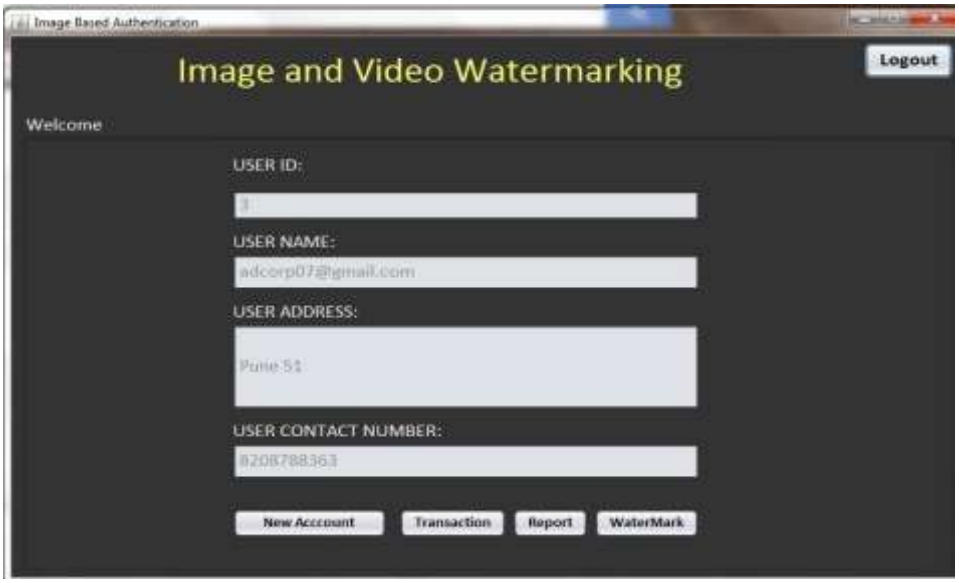

Fig 4 Account

In the above Fig 4, the proposed scheme is successfully working and and the user can further do the transactions of payments using this proposed system. The proposed system helps in logging the user to more robust system, than the traditional login password technquies and then further enhanced using One Time Password.

V. CONCLUSION

From the proposed system, we can conclude it is more reliable and stable than the traditional systems used. Comparatively it can be seen that the system communicates efficiently with the user and the portal and gives us far better security solutions for having data integrity. The system shows us that the visual cryptography is more reliable than the old methods, and can be more enhanced in the near future. The various algorithms used like KNN sharing, VSS and various watermarking techniques can be seen improving the data confidentiality along with information security. Android and iOS apps can be the future technology which makes it easier for the people to use enabling more mobile solution. The implementation of a remote and a stable system using the smartphone operating systems can make sure that the proposed system can be implemented in a faster and wider geographical area. The faster implementations of quantum computing will further help the proposed scheme to enter the new technologies and thus provide further encryption and secured methods for payment.

REFERENCES

[1] Sadaf Bhukari, Muhammad Shoaib Arif, M.R. Anjum, Samia Dilbar, "Enhancing security of images by Steganography and Cryptography techniques" The Sixth International Conference of Innovative Computing Technology (INTECH), 2016.

[2] Morteza Heidari, Nader karimi and Shadrokh Samavi, " A Hybrid DCTSVD Based Image Watermarking Algorithm" 24th Iranian Conference on Electrical Engineering ICEE,2016.

[3] Arisudan Tiwari, Anoopa Arya, Shubham Shukla, " Digital Watermarking Encryption and Decryption Using DWT" International Research Journal of Engineering and Technology (IRJET) Volume 2 Issue 2, May 2015.

[4] Rupali Jain, Jayshree Boadhh, " Advances in Digital Image Steganography", 1st International Conference on Innovation and Challenges in Cyber Security (ICICCS), 2016.

[5] Palak Patel, Yask Patel, "Secure and authentic DCT image steganography through DWT-SVD based Digital Watermarking with RSA encryption", Fifth International Conference on Communication Systems and Network Technologies, 2015.

[6] Ravi K Sheth, Dr. V V Nath, "Secured Digital Image Watermarking with Discrete Cosine Transform and Discrete Wavelet Transform method " International Conference on Advances in Computing Communication & Automation (ICACCA), Spring, 2016.

[7] Vaibhav P. Sapkal, Pooja V. Pandhare, Mahesh V. Somsetwar, Monali A. Teke, Sonali Patil, "Image Security Using Visual Cryptography and Watermarking for Multiple Data Owners" International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 1, January 2015.

[8] E. Kalaikavitha, Juliana Gnanaselvi, "Secure Login Using Encrypted One Time Password (Otp) and Mobile Based Login Methodology" Research Inventy: International Journal Of Engineering And Science Vol.2, Issue 10, April, 2013.

[9] Yun Huang, Zheng Huang, Haoran Zhao, Xuejia Lai, "A new One-time Password Method " International Conference on Electronic Engineering and Computer Science, 2013.

[10] Lavisha Sharma, Anuj Gupta "Image Encryption Using Huffman Coding for Steganography, Elliptic Curve Cryptography and DWT for Compression" International Journal of Advance research, Ideas and Innovations in Technology, Volume2, Issue5, 2016.

[11] Cryptography and Network Security (Principles and Practices)-Fifth Edition by William Stallings.

[12] Moerland, T., Steganography and Steganalysis, Leiden Institute of Advanced Computing Science, www.liacs.nl/home/tmoerl/privtech.

[13] Introduction to NetBeans, https://netbeans.org/community/index.html.

