ISSN 2395-1621

An Imroved Method For LSB & BPCS Using Visual Crptography

[#1]Tamboli Jannat, [#2]Kurapati Varsha, [#3]More Rani, [#4]Mayank Bhaskar

[1]tambolijannat@gmail.com,
[2]vrshkurapati@gmail.com,
[3]rani.more371@gmail.com,
[4]mayank.sinha024@gmail.com

[#1234]SAOE Kondhwa, SP Pune University
S.No-40/4A,Kondhwa(Bk),Saswad Road,,Pune – 411048

ABSTRACT

Steganography is one of the most powerful techniques to conceal the existence of hidden secret data inside a cover object. Images are the most popular cover objects for Steganography and in this work image steganography is adopted. Embedding secret information inside images requires intensive computations, and therefore, designing Steganography in hardware speeds up Steganography. There are several techniques to conceal information inside cover-image. The secret bits are written directly to the cover image pixel bytes. Consequently, the spatial domain techniques are simple and easy to implement. In this work, a new technique of LSB steganography has been proposed which is an improvised version of one bit LSB technique.

Keywords: Image hiding; information security; secret key; LSB; encryption

ARTICLE INFO

Article History

Received: 3rd December 2016

Received in revised form :

3rd December 2016

Accepted: 6th December 2016

Published online :

6th December 2016

I. INTRODUCTION

Image information as the main source for people obtaining information from the world, and as sociated information hiding technology is increasingly becoming an important research field of information security [1]. Among them, the least significant bit (LSB) embedding algorithm because of its features such as simple algorithm, encryption fast, easy to implement, a large amount of hidden, although it is one of the most common algorithm [2], still occupies an important position in the field of information hiding and LSB algorithm and its derived algorithm are mostly used on the Internet common steganography software. In this paper, a new method is proposed, that uses text based steganography and visual cryptography, which minimizes information sharing between consumer and online merchant but enable successful fund transfer from consumer's account to merchant's account thereby safeguarding consumer information and preventing misuse of information at merchant side. The method proposed is specifically for E-Commerce but can easily be extended for online as well as physical banking.

II. STEGANOGRAPHY AND VISUALCRYPTOGRAPHY

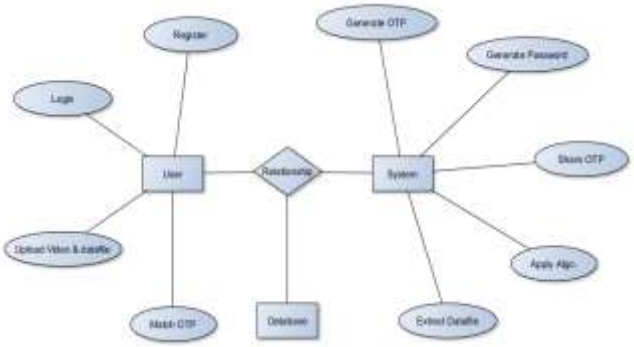
Steganography is the art of hiding of a message within another so that hidden message is indistinguishable. The key concept behind steganography is that message to be transmitted is not detectable to casual eye. Text [4], image [5], video [6], audio [7] are used as a cover media for hiding data in steganography. In text steganography, message can be hidden by shifting word and line [4], in open spaces [8], in word sequence [9]. Properties of a sentence such as number of words, number of characters, number of vowels, position of vowels in a word are also used to hide secret message. The advantage of preferring text steganography over other steganography techniques is its smaller memory requirement and simpler communication [10]. Visual Cryptography (VC), proposed by Naor et al. in [11], is a cryptographic technique based on visual secret sharing used for image encryption. Using k out of n (k, n) visual secret sharing scheme a secret image is encrypted in shares which are meaningless images that can be transmitted or distributed over an untrusted communication channel. Only

combining the k shares or more give the original secret image.

III. LITERATURE SURVEY

visual cryptography focuses on the security aspects to safeguard the secret image from two or morecover images so that any attacker cannot retrieve any data. Naor and Shamir proposed the fundamental model of the visual cryptography, starting from their many visual cryptographic methods been evolving day by day Du-Shiau Tsai et al have jointly proposed a secret image sharing method for the color images with the size constraint .the concept carries by the neural networks along with the variant visual secret sharing. The main advantages of this scheme are, it supports the 24 bit color secret image, Size constraint, increased number of quality in Camouflage images, performance of bandwidth and effective memory area, Low computation time and proves its feasibility with very good PSNR value of the reconstructed image power. Results.T.H. Chen, K.H.Tsao has published a paper called Visual secret sharing by random grids. They have proposed n out of n and 2 out of n secret image sharing schemes which is based on the Random Grids .the main advantage in this technique is here there is no pixel expansion during encryption or decryption

IV. ARCHITECTURE



In this system the data file will be embedded using image as key into the video file and sender sends this file to the receiver and the receiver extracts the data file by using the image as a key. We provide the image based authentication that can do login. Password image is generated. In this system there will be the two users, one receiver and second is sender. Sender will send the data with video that contains the embedded image. Receiver will retrieve the data by sending the image as key and then image key is matched and the data is retrieve and stored in to the f User registration contains the image as password and the image password splits into the two parts using K-N Sharing algorithm.In user authentication user is sent a Share (part of image) and share contains the watermark text for matching.If image match found next step is OTP sending on to mobile number.If OTP is matched, then the bank system starts, that contains the functionality of video watermarking.Comparison between the LSB, RSA, BPCS methods.

V. CONCLUSION

The image hiding method in this paper combine the cryptography and information hiding. On the one hand, by using information hiding does not change the visual characteristic of cover image, we can embed secret information in another public image and transfer. On the other hand, by using digital signature and encryption technology of cryptography, we can make the unauthorized users can not know the location of the embedded secret information, so that the secret information cannot be extracted. The effective combination of the above two means further improves the security of information hiding. We select encrypt the control message which determines the embedding position rather than the image or messages to hide because the process of the former is more simple, on the other hand the former also ensures the visual characteristics of the embedded information. In this paper, we improve the security on the basis of the traditional LSB information hiding, and join the identity authentication to prevent the forgery of hidden information. But there is no further research on the steganalysis. In the future, for improving this method, we must continue to study the related analysis of the hidden.

REFRENCES

[1] M. Naor and A. Shamir, “Visual cryptography,” in Proc. Eurocrypt’94LNCS 950. 1995, pp. 1–12.

[2]G. Ateniese, C. Blundo, A. De Santis and D. R. Stinson, Visual cryptography for general access structures, Inform. Computation, Vol. 129, No. 2 (1996) pp. 86–106.

[3]M. Nakajima and Y. Yamaguchi, “Extended visual cryptography for natural images,” in Proc. WSCG Conf. 2002, 2002, pp. 303–412.

4[]Stefan Droste, “New results on visual cryptography,”CRYPTO ’96 Springer-Verlag LNCS, vol. 1109, pp. 401-415, 1996.

