VISUAL CRYPTOGRAPHY FOR BANKING APPLICATION

Ashwini Thaware[1],Jyoti sahu[2],Kalyani Thakare[3],Shipra Khedikar,Supriya[4]

DEPARTMENT OF COMPUTER TECHNOLOGY
K. D. K. COLLEGE OF ENGINEERING
Sahu.jyoti1992@yahoo.in

ABSTRACT-

In this paper a novel (2, n) visual cryptographic scheme has been proposed which may be useful in banking operations in the "either or survivor" mode where n is the number of generated shares, from which n-1 is the number of account holders in an account and one share should be kept to the bank authority. In this technique one account holder should stack his/her share with the share of the bank authority and the secret image for user authentication will be revealed. In this technique two consecutive pixels are taken as the one time input for the share generation process. This technique generates shares with less space overhead compared to existing techniques and may provide better security. It is also easy to implement like other techniques of visual cryptography.

In modern years steganography is playing a significant role in secure communication. It is a technique of embedding secret information into cover media (image, video, audio and text) such that only the sender and the authoritative receiver can detect the occurrence of hidden information. The two essential properties of steganography are good visual imperceptibility of the payload which is crucial for security of hidden communication and payload is essential for conveying huge quantity of secret information. Steganography has to satisfy two requirements, one is capability and the other is transparency. Capability means embedding large payload into media. Transparency means an ability to prevent distinction between stego and cover image by statistical analysis. Earlier they have used least significant bit (lsb), the simplest form of steganography. In lsb method, data is inserted in the least significant bit which leads to a negligible change on the cover image that is not visible to the naked eye. Since this method can be easily cracked, it is more exposed to attacks. In the proposed system we propose spatial domain steganography using 1-bit most significant bit (msb) with confused manner.

KEY WORDS: LEAST SIGNIFICANT BIT (LSB), MOST SIGNIFICANT BIT (MSB), STEGANOGRAPHY,VISUAL CRYPTOGRAPHY, SHARE.

INTRODUCTION

The volatile growth in modern communication like wireless networks and the internet requires security to protect data, resources and to guarantee the authenticity from network based attacks. The two ways of providing security are cryptography and Steganography. The cryptography technique provides solution by scrambling of data with an encryption key. However in this technique the language of the plaintext is known and easily recognized, hence an intruder can suspect encrypted secret information. Steganography is the art and science of writing hidden messages in such a way that no one, except the sender and anticipated recipient, suspects the existence of the message, a form of security through anonymity. Steganography is a term derived from the Greek word Steganos which means covered or secret and graphie means writing or drawing i.e., covered writing. Steganography prevents the intruder from suspecting the secret information inthe cover object. The cover objects are digital files like Images, Video clips, Text, Music, Sound and other digital mediums. The text Steganography is the most difficult technique due to lack of redundant information in a text file compared to an image or a sound file. Digital images are of more concern for Steganography because images contain more redundant information.

Visual cryptography

Visual cryptography is a new type of cryptographic technique in which no cryptographiccomputation is needed at the decryption end. In this technique text or picture should be fed as adigital image in the system

as the input and the system generates ‘n’ (2_n) numbers of differentimages (called shares), look like images of random noise. Among ‘n’ number of shares user hasto stack ‘k’ number of shares, where 2_k_n, to reveal the secret image.The remaining portion of this paper has been organized as follows. Section 2 gives some

basicdefinitions of visual cryptography. Section 3 presents a brief overview of the related works.Section 4 describes the proposed technique. An example of the share generation process of theproposed technique is presented in the Section 5. Analysis of the performance of the proposedtechnique is presented in the Section 6. Section 7 draws the conclusions of the work.

2. SOME BASIC DEFINITIONS

Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used.
Visual Cryptography uses two transparent images. 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 .

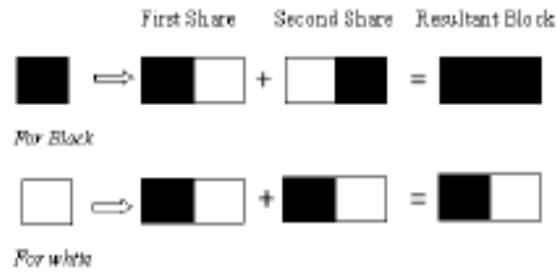
Steganography
Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. Images are the most popular cover objects use for Steganography.The properties like robustness and embedding capacity

Reversible data hiding is a newly developed branch in data hiding researches. The previous techniques only
hide and extract data from host images but reversible data hiding gives us hidden data back as well as host
image with perfect recovery [1]. The histogram based reversible data hiding techniques give minimum side
information but less data capacity. The difference expansion techniques used for hiding data gives high data
capacity but overhead of side information. So, difference expansion quad technique used to hide more data with

should be carefully considered when designing a steganography algorithm.

2.1. (n, n) visual cryptography
In this type of visual cryptographic scheme, the system generates n (n _ 2) number of shares andall shares are needed to be stacked together to get back the secret information.

2.2. (k, n) visual cryptography
1: Each Pixel is broken into two sub pixels as follows.



2: Each pixel is broken into four sub pixels as follows.

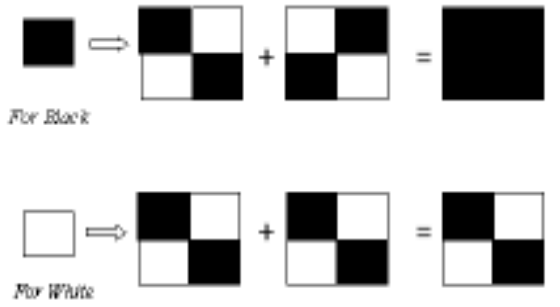
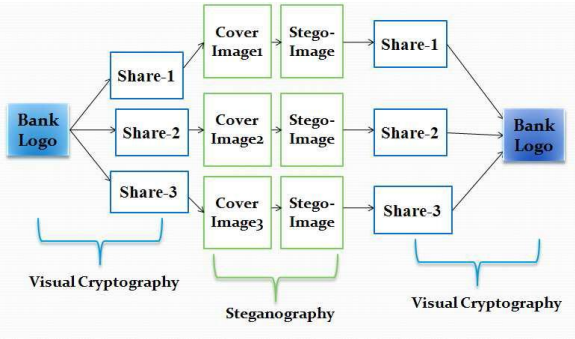


Figure 2: Visual Cryptography

ret information.

3. RELATED WORKS
less side information [2] [3].The histogram based difference expansion algorithm gives the high data capacity
with the minimum side information.
The Visual cryptography scheme (VCS) is a secure method that encrypts a secret image by breaking it into shares. These shares provide authentication [4]. A visual cryptography scheme for a set P of n participants is a method to encode a secret image into n shadow images called shares, where each participant in P receives one share. Certain qualified subsets of participants can “visually” recover the secret image, but other, forbidden, sets

of participants have no information on secrete image [5].A visual cryptography and 2D data matrix codes can be
used for authentication of ID card and ID card owner information by encrypting confidential image into noise like secure shares[6].Various other algorithms [7, 8, 9, 10] are available for different visual cryptographic schemes,where efforts have been made to enhance the security. From the literature it can also be tracedthat efforts has also been made to increase the ease of use of the visual In This paper, the combined approach of visual cryptography and steganography is used for protection of QR
code from tampering and also is used for avoid the banking frauds.
QR code is generally observed on corner of poster or webpage. There is always a threat of tampering of
original QR code with fake QR code. So instead of keeping QR code on corner of poster or webpage divide the
QR code into two shares using VC for binary images and then hide one share in cover image i.e. our poster or webpage and pass another share to the user for further authentication. Apply the extraction techniques to extract
hidden share and then pass that share to fusion technique. Only the intended user who has another share can
access QR code by passing users share to fusion step. In fusion step after overlapping both shares the required
QR code can be obtained. This technique hides QR codes presence on poster or webpage causing very little threat of tampering.
In banking application, the bank logo or key image is divided into multiple shares using visual cryptography
for colour images. Then each share is hidden into bank customer image or cover image using steganography
technique. Then at the time of access of particular joint account by multiple account holders extract each
customer share using extraction technique of steganography and overlap the customer shares to get bank logo or
key image. Then comparison can be made with certain threshold and then decision can be taken whether access is allowed or is denied. Depending on presence of number of customers the access permissions are given using k
out of n visual cryptography schemas for colour images.



4. THE TECHNIQUE

Proposed technique considered two consecutive pixels as the one time input in thesource image and as a result there shall be four cases in input. These are as follows:
(i) Black and Black, (ii) Black and White, (iii) White and Black, (iv) White and White
To develop a (2, n) visual cryptographic scheme two things are considered as majorpoint of references[12]. These are:(i) Hamming weight of every block in each share should be the same.
(ii) Hamming weight of a black block will be greater than the other blocks inthe stacked shares.
Let N is the number of participants (i.e no. of account holders). m=integer part of (n/2),where n= number of total shares. The bank authority has to select the value of n, suchthat the relation nCm _ min{(N+1)} (where C represents the combination operation)holds. Hamming weight of each block of each share (H) = Integer part of (nCm)/2;International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.4, October 2010122Now Let us consider the four possible cases of input pixels:
(i) Black and Black: In this case arrangement of black pixels in the output
block will be different from other blocks. This ensures that after stacking
the shares, Hamming weight of the stacked black blocks will become
greater than the other blocks.
(ii) Black and White: Here the all the black pixels will be kept together from
the first position of the output block.
(iii) White and Black: Where the all the black pixels will be kept together
from the last position of the output block
(iv) White and White: All black pixels will be kept together in the outputblock
Now if the number of pixels in the input image is odd then the last pixel will be kept asit is in the shares.

6. PERFORMANCE ANALYSIS

From the literature study it is seen that the paper [4] developed by ChetanaHegde, Manu S, PDeepaShenoy, Venugopal K R, L M Patnaik , was an work for secure banking applicationsusing visual cryptography. Let us compare the characteristic features of the proposed algorithmwith the algorithm developer by ChetanaHegde et. al.Table 1. Performance analysis**Features Algorithm proposed by ChetanaHegde et. al.[4]Proposed Algorithm**Type of the algorithm (2,2) visual0cryptography(2,n)visual cryptographyApplicability Maximum number ofaccount holder is oneNo limit in the number ofaccount holderPixel expansion 4 times variableNumber of pixelper inputone twoType of the algorithm (2,2) visualcryptography(2, n) visual cryptographyTable 1 presents the comparison of some salient features between the proposed algorithm andthe algorithm proposed by ChetanaHegde et. al. [4] where it is clear that in case of proposedtechnique the space overhead has been reduced as two input pixels are clubbed together in inputand taken as single pixel for share generation and the propose algorithm is more useful thanprevious one.

APPLICATIONS OF STEGANOGRAPHY

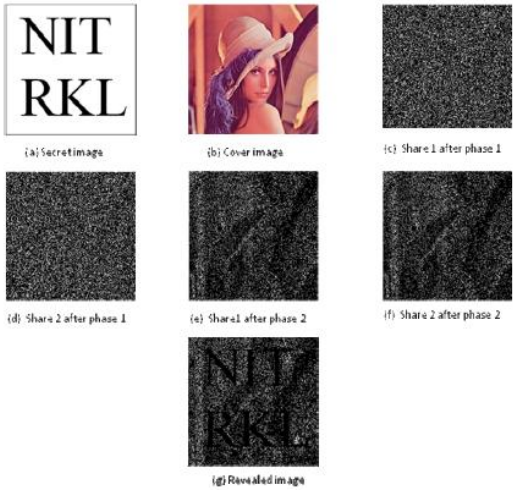
1 Enables secret communication

2 Compliments regular encryption: Hard to break: need to first find the encrypted secret text then it needs to be decrypted.

3 Remarkable use in Military Applications.

EXISTING SYSTEM

Least significant bit (LSB) is the simplest form of Steganography. It is based on inserting data in the least significant bit of pixels, which lead to a minor change on the cover image that is not noticeable to naked eye. Since this method can be easily cracked, it is more susceptible to attacks.



DISADVANTAGES

1 We noticed that in the approach, the time taken for generating the random numbers depends on the size of the key. In our approach it means that it also depends on the cover-image size.

2 Though in LSB embedding methods data is hidden in such a way that the humans do not perceive it, such schemes can be easily destroyed by an opponent such as using lossy compression algorithms or a filtering process.

3 Any process that modifies the values of some pixels, either directly or indirectly may result in degrading of the quality of the original object.

4 LSB method has intense effects on the statistical information of image like. Attackers could be aware of a hidden communication by just checking the Histogram of an image.

5 LSB is extremely susceptible to corruption. That is, the reliability of the hidden message can effortlessly be ruined. All the attacker must do is to randomize the LSBs of the image. The intruder may not even know that it is a stego-image, but such actions would demolish the secret message.

REFERENCES

[1] Hsiang-Cheh Huang, Senior Member, IEEE, Feng-ChengChang, Member, IEEE, and Wai-Chi Fang, Fellow, IEEE, "Reversible data hiding with histogram based difference expansion for QR code applications," IEEE Transactions on Consumer Electronics, vol.57, no.2, pp. 779-787, May 2011.

[2] H. J. Kim, V. Sachnev, Y. Q. Shi, J. Nam, and H. G. Choo, "A novel difference expansion transform

for reversible data embedding," IEEE Trans. Information Forensics and Security, vol. 3, no. 3, pp. 456-465, Sep. 2008.
[3] Chandramathi S., Ramesh Kumar R., Suresh R. and Harish S., "An overview of visual cryptography," International Journal of Computational Intelligence Techniques, ISSN: 0976–0466 & E-ISSN: 0976–047 vol. 1, Issue 1, pp.32-37, 2010.
[4] D. Jena, and S. K .Jena,(2009) "A Novel Visual Cryptography Scheme", The 2009 International Conference on Advanced Computer Control, pp-207-211.
[5]OmprasadDeshmukh, Shefalisonvane, "Multi-Share Crypto-Stego Authentication System" IJCSMC, Vol. 2, Issue. 2, February 2013, pg.80 – 90.
[6] J. K. Pal, J. K. Mandal and K. Dasgupta (2010) "A Novel Visual Cryptographic Technique through Grey Level Inversion (VCTGLI)" Proceedings of The Second International conference on Networks & Communications, Chennai, India, pp. 124-133
[7] M. Heidarinejad, A. A. Yazdi,; K.N. Plataniotis, (2008) "Algebraic Visual Cryptography Scheme for Color Images" IEEE International Conference on Acoustics, Speech and Signal Processing, pp. 1761 – 1764.
[8] G.R Zhi Zhou Arce,. G. Di Crescenzo (2006) "Halftone Visual Cryptography". IEEE Transactions on Image Processing. , Volume: 15, Issue: 8pp- 2441-2453.
[9] A. Houmansadr, S. Ghaemmaghami, (2006) "A Novel Video Watermarking Method Using Visual Cryptography" IEEE International Conference on Engineering of Intelligent Systems, , Islamabad, Pakistan, pp 1-5.
[10] P. Geum-Dal,; Y. Eun-Jun,; Y. Kee-Young , (2008) "A New Copyright Protection Scheme with Visual Cryptography", Second International Conference on Future Generation Communication and Networking Symposia. pp. 60-63.
[11] Y. Wei-Qi, J. Duo,; M. S. Kankanhalli, (2004) "Visual Cryptography for Print and Scan Applications". International Symposium on Circuits and Systems. pp- 572-575.
[12] S. Gravano,(2001) Introduction to Error Control Codes, Oxford University Press, USA.