Volume 5, Issue 1, January 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Image Security Using Visual Cryptography and Watermarking for Multiple Data Owners

Vaibhav P. Sapkal[1], Pooja V. Pandhare[2], Mahesh V. Somsetwar[3], Monali A. Teke[4], Prof. Sonali Patil[5]

[1, 2, 3, 4]Student, SCOE, Sudumbare, Pune, India

[5]Assistant Professor, SCOE, Sudumbare, University of Pune, India

Abstract— In the fast technological world, many traditional security techniques are provided to secure data exchange between various devices. But the existing system does not provide much of the security to the media. In the existing system, lightweight security is used, secondly digital rights management is most important. There are multiple owners who are having equal rights for a single data; there is a need to give an equal authority to all the data owners. There is no single administrator who has all the rights to that confidential data. The confidential data should be secured in such a way that no single administrator from all the data owners will be able to get the data as a whole. The need for implementing adequate security services is increasing so that the confidential data cannot be accessed by unauthorized people. To address the above challenges, we proposed the system to use both secure sharing and watermarking schemes to protect user's data. The secure sharing scheme gives the security to the data and watermarking scheme will authenticate the particular data to the individual owners. Thus our proposed approach achieves good security performance.

Keywords— Visual Cryptography, RSA technique, Alpha Channel Watermarking

I. INTRODUCTION

In this new era of information technology, internet is widely used for transmitting multimedia information. When the data is confidential or secret then the security of it becomes the most important issue. While dealing with secret images security is necessary otherwise attackers can utilize that data for their benefits. To deal with such security issues of the confidential data many secret sharing schemes have been developed. 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.

In this paper, visual cryptography is used to provide equal digital right to all the owners. To provide more security during transmission of the shares, encryption can be applied on each share. Watermarking is applied on the shares to authenticate each share with its owner. The rest of the paper is organized as follows: Section II describes the literature survey of visual cryptography, encryption and watermarking techniques. Section III shows architecture of the system. Section IV provides the basic algorithm used in the proposed system, followed by the conclusion in the section V.

II. LITERATURE SURVEY

A. Visual Cryptography

Cryptography is the best technique to secure confidential digital data which is used to send and receive those assets in the encrypted format. Naor and Shamir [1] pointed out visual cryptographic scheme for maintaining confidentiality and safe sharing of secret images in ensured channels. This technique uses binary images which consist of black and white pixels. According to Each pixel value in binary image, SH1and SH2 is encoded. By superimposing these shares original binary image can be visible.

Wu and Chen [2] proposed new visual cryptographic scheme to encode two binary images into different two shares. They hided secret into two random shares, say P and Q. First secret (P) can be revealed by stacking both shares and second share (Q) can be revealed by rotating one of them by some angle in anti-clockwise direction and stacking both of them. Borchert [3] introduced Segment based visual cryptography which can be used only for encryption of messages containing alphanumeric symbols. Segment based visual cryptography have great benefit over pixel based visual cryptography when it is used in online banking security and key distribution among the participants [4]. Bhasakara Rao et al. [5] introduced secret sharing scheme in which secret shares are hidden in meaningful cover images. So secret is concealed from network intruders. This technique performs XOR operation on cover image. Sian-Jheng lin et al., [6] introduced (k, N) visual cryptographic scheme to divide secret image among N shares. Secret image is revealed by superimposing at least k out of N shares. Shares less than k cannot reveal original secret image.

Extended visual cryptographic scheme not only generates N shares but also these shares are visible to naked eyes. In other words shares encoded by this scheme are meaningful images. These shares are in gray scale or halftone gray scale images. Hyper graph coloring technique is used to generate meaningful images. Figure 1 shows general classification of visual cryptography.

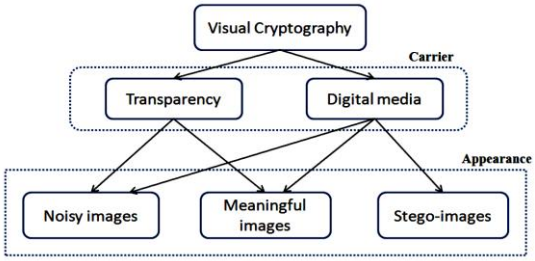

Figure 1: Classification of visual cryptography

Kai-Hui Lee et al., [7] proposed Natural image-based VSS scheme (NVSS) in which N-1 innocuous natural images are used to extract features and these features are encrypted with N secret images or shares. These shares may be noisy or meaningful shares. NVSS scheme resists the transmission risk.

B. Watermarking

Now a day's internet is being a popular medium to transfer the digital information from one place to another. In the mean time of the transmission, illegal copies of the original data can be made to make changes or to interchange the information. It can be difficult to distinguish between the original information and its copy as no security is provided to the data. Digital Watermarking technique is used to identify whether the data is original or duplicate. It provides the ownership and secures it from illicit copies.

Digital watermarking is a process of embedding some pattern/data in the digital information to verify authenticity, ownership of the data [10]. The digital information can be in the form of image, video, audio, or text, etc. The digital information in which the watermark to be embedded is known as the host. The embedded watermark can be a logo or any useful information which proves the ownership of the data. Digital watermarking has various applications such as copyright protection, authentication, covert communication, source tracking, broadcast monitoring, etc.

Digital watermarking can be visible or invisible. In visible watermarking the watermark to be embedded in the host is purely visible to the users. Whether in the case of invisible watermarking the pattern or the watermark is in the hidden format that means the watermark is not visible to the users of the data. This type of watermarking technique can be useful in the covert communication between the people.

C. Encryption and Decryption Algorithm

Security is the most important issue when the data is confidential. The data should be converted in such a form so that anyone cannot retrieve it except the authorized people. Encryption is the process of converting the plain text into the cipher text. Decryption is the reverse process which converts the cipher text to the original plain text. Encryption and decryption algorithm requires two inputs, plain text or cipher text and the key.

The encryption algorithms are classified in two types based on the key distribution: In Secret key encryption algorithm, the encryption and decryption is done using the same key and the key must be securely distributed using secured channel. In Public key encryption algorithm, the encryption is done by one key which is called as public key and decryption is done by another key which is the private key.

RSA is the public key encryption algorithm proposed by Ron Rivest et al, [11] in which there is no need to use another secure channel for key distribution to the participants. The public key used for encryption is known to everyone and the private key is known to the recipient participant itself. Even if the intruder is having the public key he cannot determine the decryption key to get the original data. It is very tedious for intruder to break RSA algorithm because, it uses factoring large prime numbers to generate public and private key. RSA algorithm is widely used when the data is confidential or more sensitive such as government policies, military purpose, etc.

III. ARCHITECTURE

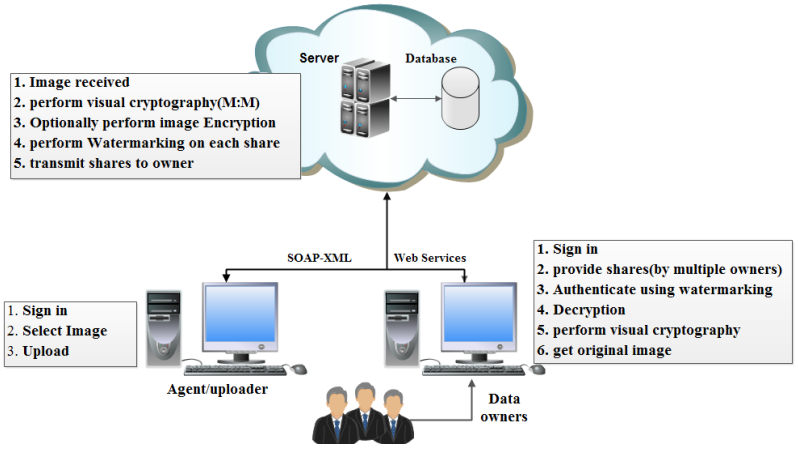

Figure 2: System Architecture

Figure 2: Shows the System architecture consisting of three parts described as follows:

A. Registration Phase

In the registration phase, along with the personal information, password, watermark details and number of owners of the image must be provided by Uploader. All the information is stored in database. Uploader and data owners must register to the cloud. No further processing can be done without registration.

B. Processing Phase

Uploader uploads image to the cloud. Cloud splits the received image into N number of shares defined by Uploader. If Uploader wants to provide more security to the shares then these shares can be encrypted. For authentication of each share and its owner, watermark is applied on these shares. These shares are transmitted to its particular owner via E-mail.

C. Reverse Processing Phase

To retrieve the original image, the data owners must provide their shares to the cloud for further processing. These watermarked shares are checked for authentication of the owner. Valid shares are then decrypted using the key provided by the owner if encryption is applied on the shares. Once all the shares are decrypted, these shares are superimposed to obtain the original secret image. Shares less than N cannot reveal the secret; all the shares are required to obtain the original secret image.

IV. BASIC ALGORITHM

In this section, the basic algorithms used in the proposed scheme are described.

Algorithm 1: Encryption.

RSA Algorithm includes three steps: Key generation, Encryption and Decryption described as follows:
Key Generation: The keys for algorithm are generated using following steps:

1. Select two different large prime numbers A and B. The numbers can be selected randomly and they should be of equal bit length.
2. Calculate n=A*B; n is used as modulus for both keys that is public and private key.
3. Calculate the Euler's totient function Φ as Φ(n)=(A-1)(B-1).
4. Select a number *e* such that $1<e<\Phi(n)$ and GCD(Φ(n),*e*)=1; *e* and Φ(n) must be co-prime numbers.
5. Calculate $d=e^{-1}(\text{mod } \Phi(n))$, where, *d* is the multiplicative inverse of *e* mod Φ(n).

Encryption:

1. Select a message M, such that M<n
2. Calculate cipher text C, $C=M^e \pmod n$.

Decryption:
Select the cipher text C, and recover the message M, $M=C^d \pmod n$.

Algorithm 2: Watermark Embedding.

Input: Host color image I, color watermark W, and a key K.
Output: Watermarked image I'.
Steps:

1) Transform the host image I into a PNG image by adding the alpha channel plane A, and assign the values of pixels in A to 0.
2) Select a region R, where watermark W is to be embedded, in the host image I and replace the pixel's color values in R with the values in W, and for every replaced pixel get the RGB value of 24 bits to form data string S.
3) Assign the values of the pixels in A to 255 underlying the watermark in R.
4) To randomize the order of the bit sequence to get S' of the bit sequence in S use a key K.
5) Take 3 bits at a time from S' and an alpha pixel from A, as s and p, respectively , and follow the steps:
   a. Convert s into a decimal number s'.
   b. If p is not equal to 255, replace p with s'; otherwise, take the next alpha pixel from A.
6) If there are bits in S' to be embedded, then go to Step 5; otherwise, continue.
7) Add 247 to all pixels in alpha excepting those having value 255 in A; getting the new values which are in the range of 247 to 254 and denote the resulting A, containing the alpha values from 247 to 254 and those having value 255 set in Step 3, to be A'.
8) Obtain the resulting Image with the embedded W together with the A' as the desired watermarked image I'.

The data required for the removing the watermark from the watermarked image will be obtained from the alpha channel plane. After the removal of the watermark, the alpha channel is eliminated in order to obtain the original color host image in the reverse process.

V. CONCLUSION

In this paper, we proposed 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.

REFERENCES

[1] Moni Naor and Adi Shamir, "Visual cryptography". In Proceedings of the advances in cryptology- Eurocrypt, 1-12,1995.

[2] C.C. Wu and L.H. Chen, "A Study On Visual Cryptography", Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998.

[3] B. Borchert, "Segment Based Visual Cryptography", WSI Press, Germany, 2007.

[4] Indrakanti S. P. and Avadhani P. S. "Segment based Visual Cryptography for Key Distribution". IJCSES Vol. 3, No. 1, Feb 2012.

[5] S. S. Hegde, Bhaskar Rao, "Cloud Security Using Visual Cryptography", International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012,pp.9-13.

[6] Sian-Jheng Lin and Wei-Ho Chung, "A Probabilistic Model of (t,n) Visual Cryptography Scheme With Dynamic Group", IEEE Transactions on Information Forensics and Security, vol. 7, No. 1, February 2012, pp.197-207.

[7] Kai-Hui Lee and Pei-Ling Chiu, "Digital Image Sharing by Diverse Image Media", IEEE Transactions on Information Forensics and Security, vol. 9, No. 1, February 2014.

[8] Che-Wei and Wen-Hsian "A new lossless visible watermarking method via the use of the png image," IASTED_ASC, 2012.

[9] T. Y. Liu and W. H. Tsai, "Generic lossless visible watermarking a new approach," IEEE Transactions on Image Processing, 19(5), 2010, 12241235.

[10] M. Natarajan and Gayas Makhdumi "Safeguarding the Digital Contents: Digital Watermarking," DESIDOC Journal of Library & Information Technology, Vol. 29, No. 3, May 2009, pp. 29-35.

[11] Rivest, R.; A. Shamir; L. Adleman (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," PKCS#1, ANSI X9.31, IEEE 1363.

[12] F. Amin, A. H. Jahangir and H. Rasifard, "Analysis Of Public key Cryptography For Wireless Sensor Networks Security," In Proceedings of World Academy of Science, Engineering and Technology, ISSN 1 307-6884, 2008.

