ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

Secret Data Transmission Using Symmetric Key, Visual Cryptography and Steganography

Shalaka Dange[1], Prof. R. M. Mukhedkar[2]

P.G. Student, Department of E&Tc Engineering, Dr. D. Y. Patil COE, Ambi, Pune, India.[1]

Professor, Department of E&Tc Engineering, Dr. D. Y.Patil COE, Ambi, Pune, India.[2]

ABSTRACT:Internet has become a primary source of transmitting confidential or secret data such as military information, financial documents, etc. In such cases, techniques devoted to protect such kind of information are needed and they play an important role in providing confidential and secure transmission over network. Visual Cryptography is also one of them which is used to hide secret visual information (such as image, text, etc) in which secret sharing scheme is used. Secret sharing is used to encrypt a secret image into customized versions of the original image.In this paper,we are suggesting one new method in which a symmetric secret key is used to encrypt the image and then secret shares are generated from this image using Novel secret sharing technique with steganography. So, finally this method will produce meaningful shares and use of secret key will ensure the security of scheme. This scheme can become a reliable solution suitable for today's authentication challenges.

KEYWORDS*:*Visual cryptography, Secret sharing steganography

I. INTRODUCTION

The Internet has become a popular communication network where the distribution of multimedia content, confidential data such as military information, financial documents, etc. has become a common practice. But, over Internet the information is viewed to many users. Hence, now the security of visual information has become more and more important in many real applications. To fulfill such an increasing demand of security, many security providing tools are there in this scenario and Visual cryptography is one of them. This is introduced by Naor& Shamir in 1979 to provide confidentiality and security when secret visual information is transmitted through unsecured communication channels. Using secret sharing concepts, the encryption procedure encrypts a secret image into number of shares (printed on transparencies) which can be distributed among group members or transmitted or distributed over number of an untrusted communication channels such that only stacking of these shares can reveal the information otherwise not. Then the idea of secret sharing was also separately proposed by Adi Shamir and G. Blakley in 1979. In 1983 another method of secret sharing was proposed by Asmuth and Bloom. Shamir's scheme is based on Polynomial Interpolation. Blakley secret sharing is based on hyper plane geometry. Asmuth-Bloom secret sharing scheme is based on Chinese Remainder theorem. Then there are many methods to protect sensitive data in image and Steganography is also one of them. This method hides a secret message in a innocent cover medium which could be a digital image,video, audio; etc. but, the weakness of this technique is that an entire secret data is kept in a single cover medium and if this cover medium get lost or corrupted then that hidden data may also get corrupted. In 2004, Lin and Tsai proposed a method that used Steganography for generation of meaningful shares with secret image sharing. This scheme also used polynomial-based secret sharing approach proposed by Shamir which leads to high computational complexity. As the decryption process is done by human visual system, secret information can be retrieved by anyone if the person gets at least k number of shares. So that simple visual cryptography became very insecure. In this paper, a new idea is suggested which is a visual cryptography method different from any of the methods discussed previously. In this new method, original image having secret information is going through two levels of encryption. In first level, secret image is encrypted by using a symmetric key based visual cryptography resulting into new cipher image which is then divided into no. of meaningful shares by applying novel secret sharing with steganography algorithm.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

II. RELATED WORK

Previously, Naor and Shamir introduced secret sharing approach in 1979. Afterwards, Asmuth and Bloom proposed another secret sharing algorithm. Shamir's secret sharing scheme is based on Lagrange's Polynomial Interpolation theorem. This scheme divides a secret data image into n number of shares share1, share2.....share n and these n shares are Xeroxed onto n transparencies, respectively, and distributed amongst n participants, one for each participant. Such that: i) By superimposing any k or more shares among share i transparencies together can reveal the secret information. ii) Less than k shares reveals no information about the secret share. This technique is called (k, n) threshold secret sharing. The (k, n) secret sharing comes from the concept that k pointsare necessary to define a polynomial of degree (k−1). Blakley Secret sharing scheme is based on hyper plane geometry. It is known that non-parallel planes intersect at a single specific point. This secret sharing scheme says that: i) Secret is a single point in m-dimensional space. ii) Share corresponds to a hyper plane. Iii) Intersection of thresholdplanes gives the secret. iv) Less than threshold planes will not reveal secret. In Asmuth-

Bloom secret sharing scheme shares are created on the basis of Chinese Remainder theorem. In this, shares are generated by reduction modulo operation and the secret is recovered by solving the system of congruence using the Chinese Remainder Theorem. Previously, visual cryptography was restricted to binary images and because of this; it became inefficient in real time applications. Chang- ChouLin, Wen-Hsiang Tsai proposed visual cryptography for gray level images by dithering techniques. A dithering technique is used to convert gray level images into approximate binary images. Then shares are created by applying existing visual cryptography schemes for binary images. The limitation in this is that all generated shares are random patterns carrying no visual information, look like noisy images. This scheme is still satisfactory in the aspects of increase in relative size and decoded image quality, even when the number of gray levels in the original image still reaches 256. Halftone Visual Cryptography was proposed by Zhi Zhou, Gonzalo R. Arce, and Giovanni Di Crescenzo. In this paper, a general framework of halftone visual cryptography is proposed by which visually pleasing halftone shares, carrying significant visual information are generated. Applying the rich theory of blue noise halftoning into the construction mechanism of conventional VC, the obtained visual quality is better than that attained by any other available VC method. Extended visual cryptography for natural images first introduced by Naor which constructs meaningful binary images as shares as shown in fig. 1 and enables the contrast enhancement, where a simple example of (2, 2)-EVCS was presented. This can be treated as a technique of steganography.

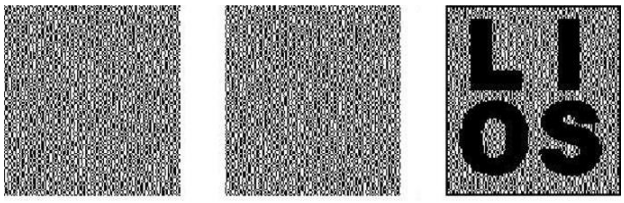

Fig.1. Example of traditional (2, 2)-VCS

There are many EVCSs proposed in the literature. Droste, Ateniese, and Wang also proposed three EVCSs, respectively, by manipulating the share matrices. Nakajima also proposed a (2, 2)-EVCS for natural images. Then afterwards Embedded Extended Visual Cryptography Scheme was proposed by Feng Liu and Chuankun Wu and realized by embedding the random shares into the meaningful covering shares as shown in Fig.2. An Extended Visual Cryptography Algorithm for General Access Structures was proposed by Kai-Hui Lee and Pei-Ling Chiu. This approach consists of two phases. In the first phase, they construct meaningless shares using an optimization technique and the construction for conventional VC schemes. In the second phase, cover images are added in each share directly by a stamping algorithm. The experimental results indicate that the display quality of the recovered image is very close to that obtained using conventional VC schemes. Liu, C.K. Wu X.J. Lin, proposed a new approach on visual cryptography for colored images. They proposed three approaches as follows: In first, they realize the color VCS as to print the colors in the secret image on the shares directly similar to basic model.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

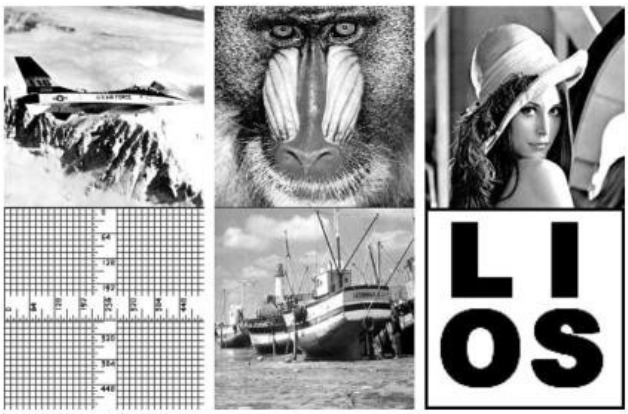

Fig. 2: Original share images (airplane, baboon, Lena, ruler, and boat) and the secret image.

It reduces the quality of the decoded color image. In second, a color image is converted into black and white image or the three color channels (red, green, blue or equivalently cyan, magenta, yellow), respectively, and then apply the black and white VCS to each of the color channels which results in reduction in quality of the image due to halftone process. And e of JPEG to all the created share images.in final approach they utilizes the binary representation of the color of a pixel and encrypts the secret image at the bit-level which results in better quality than first two but requires devices for decryption. Shared Key Encryption of JPEG Color Images was proposed by SubramaniaSudharsanan. This paper mainly focuses on {2, 2} shared encryption method for JPEG images. This method creates two shares of JPEG or any format image. This method uses the quantized DCT coefficients in the JPEG representation for generation of shares. These shares are used to reconstruct the original quantized DCT coefficients during decryption.

III. PROPOSED CONCEPT

To transmit or store an image in a safer way against unauthorized persons, there are at least three possible major approaches: encryption with keys, hiding the image in other media or objects i.e, steganography, sharing of image among distinct parts i.e. visual cryptography. Combination of these three major approaches is also possible. Secret sharing of image or encryption of image with the help of key produce images which looks like noisy images or textured image. So, there may be chances that attacker may come to know that this image is surely encrypted image or carrying something secret data and if he can't get access to that secret data, he will try to destroy it. For dealing with such problems, one can use steganography which hides the secret information or image into one innocent cover image that the attacker may fails to guess whether this image contains secret information. But, in this entire secret data is kept in single cover image. So, in this also there may be a chance that if this image may get lost or corrupted. For such problem, a method which uses steganography for generation of meaningful shares can be a solution. So, we proposed a new scheme that will overcome such problems associated with secret image encryption. Objective of proposed scheme is to design an encryption/decryption algorithm that efficiently provides high level security for visual information from illicit attacks.

A. ENCRYPTION PROCESS:

The encryption process involved in our proposed scheme is as shown in Fig.3 which includes firstly encryption of secret image by symmetric key based visual cryptography algorithm which results in cipher image which looks like noisy image and then secondly, by applying secret sharing algorithm with steganography to key encrypted image which results in meaningful shares. Advantage of this combined version of two schemes is that key encryption before secret sharing of image will give additional security and use of steganography in secret sharing can provide additional security as it befools the attacker's eye without computational overhead. In Encryption process, the secret image is first of all treated with symmetric key. This symmetric key is to be generated with the help of symmetric key generation algorithm. After applying key, cipher image is generated which is then divided into n number of meaningful shares by applying Novel secret sharing with steganography algorithm.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

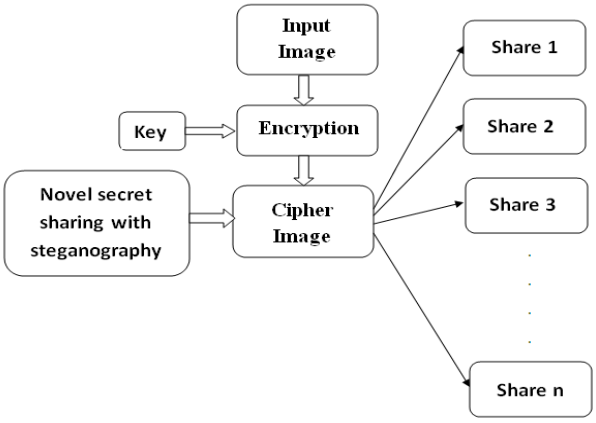

Fig.3. Encryption Process

B. DECRYPTION PROCESS:

At intended receiver, when that n no. of stego share images will get received then decoding of stego share images will be carried out and original secret image will be recovered. Thus, decryption process consists of steps same as performed in encryption process but exactly in reverse order. In Decryption process, out of n received stego share images firstly select any k no. of share images which are to be stacked.

REFERENCES

1. G. Blakley, "Safeguarding cryptographic keys," Proc. The National Computer Conference, NJ, USA, 1979.
2. Shamir, "How to share a secret," Proc. Comm. ACM, vol (2), 612-613, 1979.
3. El-Tigani B. Abdelsatir, SaharSalahaldeen, Hyam Omar and AfraHashim, " A novel secret sharing scheme from quadratic residues for grayscale images " , International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.4, J.uly 2014.
4. Kamer Kaya , Ali AydınSe|cuk, ZahirTezcan,, "Threshold Cryptography Based on Asmuth-Bloom Secret Sharing".
5. IlkerNadiBozkurt, Kamer Kaya, Ali AydınSelcuk, Ahmet M. Guloglu, "Threshold Cryptography Based on Blakley Secret Sharing".
6. Pallavi Vijay Chavan, Dr. Mohammad Atique and Dr. Latesh Malik , "Design and Implementation of Hierarchical Visual Cryptography with Expansionless Shares", International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014.
7. John Justin.M , Alagendran.B , Manimurugan.S ,"A Survey on Various Visual Secret Sharing Schemes with an Application", International Journal of Computer Applications (0975 – 8887) Volume 41– No.18, March 2012.
8. Shanu Sharma," An Implementation of a Novel Secret Image Sharing Algorithm", IJCSMC, Vol. 2, Issue. 4, April 2013, pg.263 – 268.
9. HarinandanTunga and Soumen Mukherjee," Design and Implementation of a Novel Authentication Algorithm for Fool-Proof Lock-Key System Based On Steganography and Key based Visual Cryptography using Novel secret sharing method Visual Secret Sharing Scheme", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, May 2012.
10. Nayan A. Ardak Prof. AvinashWadhe," Visual Cryptography Scheme for Privacy Protection", Nayan A. Ardak et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 2026- 2029.
11. PoonamBidgar, NehaShahare," Key based Visual Cryptography Scheme using Novel Secret Sharing Technique with Steganography", IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) eISSN: 2278- 2834,p- ISSN: 2278-8735.Volume 8, Issue 2 (Nov. - Dec.2013), PP 11-18
12. SonamSoni,", A Road Map to Visual Cryptography, Volume 5, Issue 4, 2015 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering.