ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 5, Issue 5, May 2016

A Brief Survey on Visual Cryptographic Approaches

Jaya Solanki, Mahendra K Verma

***Abstract*— Visual cryptography is a technique that encrypts visual information such as image in a way where decryption not requires a computational effort. This approach attracts a number of researchers for discovering more effective and efficient techniques. In this presented paper a survey on different cryptographic approaches of visual information is presented and some key issues are addressed on exiting visual cryptographic technique. Finally a new visual cryptographic approach is proposed that enhance the quality of encrypted image shares. Additionally future extension of the presented technique is also provided.**

***Index Terms*— Visual Cryptography, Visual Information, Encryption, Image shares, Information hiding.**

I. INTRODUCTION

The art of preserving information by transforming it into a cipher text is known as cryptography. Only those who have a secret key can decipher the original data. As the Internet and other communication techniques are growing, electronic security is becoming more important. Most of the time cryptography is used to protect electronic messages such as credit card information. There are various different kinds of cryptographic schemes and techniques are available based on the nature of Encryption algorithms that can be classified into two broad categories- Symmetric and Asymmetric key encryption [1].

A. Symmetric Encryption

Symmetric encryption is best-known technique. This technique utilized with a secret key. That can be a number or a string of random letters. This key is applied to message to transform content in a particular manner. This approach can be as simple as shifting each letter by a number of places. In this technique sender and recipient required to know the secret key to encrypt and decrypt messages [2].

***Manuscript received April, 2016*.**

***Jaya Solanki**, Computer Science, Sushila Devi Bansal College of Technology,). Indore, India, Mobile No. 7691907469.*

***Mahendra K Verma**, Computer Science, Sushila Devi Bansal College of Technology, Indore, India,*

B. Asymmetric Encryption

Exchanging secret keys among both the parties over Internet, while preventing information from falling into the wrong hands can affect the privacy and security of data thus asymmetric encryption helps to enhance the security. In asymmetric encryption there are two keys. A public key available to anyone and a private key kept secret. Any message that is encrypted by public key can only decrypted by matching private key. This means there is a way to passing public keys over the public network. A problem with asymmetric encryption is that it is slower than symmetric encryption [3].

In this study the image and text encryption scheme to manipulate information to hide them. Encryption algorithms are varying according to data formats. Therefore for encryption and decryption of two data formats are a goal in this study. In addition of that successfully data recovery from modified message is also a complex task in presence of different data formats. Therefore a new solution is tried to find.

II. VISUAL CRYPTOGRAPHY

The transmission of data over network is common activity now in these days. That enables a network user for instant access or distribution of digital data. In order to prevent data from unwanted access or intruder the cryptographic techniques are frequently used. In this presented work the visual information distribution technique is investigated in detail. For improving the security for visual information various image encryption and the visual cryptographic manner is developed in recent years.

The concept of visual cryptography is first introduced by Naor and Shamir [4]. Visual cryptography is the technique of latest technology that is used to transmit the secret information either into text or image. Secret sharing is important domain in information security. However security can be introduced in many ways such as password, information hiding, watermarking etc. But the drawback of these methods is that the secret images can be protected in single information carrier. If it lost once, the information carrier is either damaged or destroyed [5].

In basic visual cryptographic technique the data or image is converted into a number of shares. These shares are combined to each other for generating the original information or hidden data. For example there is an image I, which is converted into two shares S_1 and S_2 during

encryption process. And during the decryption of the data both the shares S_1 and S_2 are required to recover the original information. The given scheme of visual secrete sharing scheme is given using figure 1.

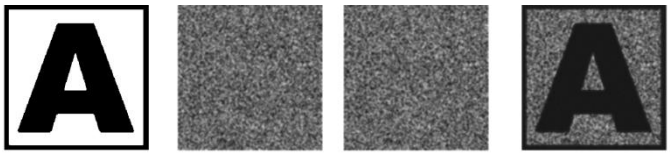

Figure 1 visual cryptography

In this given diagram the first image is original information which is required to hide. This image also termed as the secrete image. During the encryption process the image is converted into similar size shares as given two non-visual images in figure 1. Furthermore for decryption when both the shares are combined the required information is recovered as given in final image of the figure 1.

III. RECENT STUDIES

In this section the novel work in the domain of visual cryptographic technique is discussed.

A. Sharing multiple secrets in visual cryptography

The secret sharing schemes in conventional visual cryptography are characterized by encoding one shared secret into a set of random transparencies which reveal the secret to the human visual system when they are superimposed. In this paper, we propose a visual secret sharing scheme that encodes a set of $x \geq 2$ secrets into two circle shares such that none of any single share leaks the secrets and the x secrets can be obtained one by one by stacking the first share and the rotated second shares with x different rotation angles. This is the first true result that discusses the sharing ability in visual cryptography up to any general number of multiple secrets in two circle shares [6].

B. Structure Aware Visual Cryptography

Visual cryptography is an encryption technique that hides a secret image by distributing it between some shared images made up of seemingly random black-and-white pixels. Extended visual cryptography (EVC) goes further in that the shared images instead represent meaningful binary pictures. The original approach to EVC suffered from low contrast, so later papers considered how to improve the visual quality of the results by enhancing contrast of the shared images. This work further improves the appearance of the shared images by preserving edge structures within them using a framework of dithering followed by a detail recovery operation. We are also careful to suppress noise in smooth areas [7].

C. Visual Cryptography Using Region Increment- action

Region incrementing visual cryptography is used to hide multiple secrecy levels in a single image. In n level region incrementing visual cryptography scheme, image is divided in n regions. Each region consist single level information. For implementing visual cryptography in n levels we need to encode (n+1) shares in such a way so that any single share is not able to show the information and by combining any two shares, first level information would be visible. Similarly by superimposing any three shares, information up to second level could be seen. In similar way, for revealing whole information all the (n+1) shares are superimposed. These n levels are created according to user specification. In proposed scheme, user does not need to address the area of different levels manually and levels are created automatically. User needs only particular level information with a particular size of text. The traditional region incrementing visual cryptography scheme has been modified to address the problem of pixel expansion and poor contrast. In proposed algorithm, problem of pixel expansion and poor contrast has been removed and further it is modified to generate the levels automatically which is named as automatic region incrementing visual cryptography [8].

D. Halftone Visual Cryptography

Visual cryptography encodes a secret binary image (SI) into shares of random binary patterns. If the shares are xeroxed onto transparencies, the secret image can be visually decoded by superimposing a qualified subset of transparencies, but no secret information can be obtained from the superposition of a forbidden subset. The binary patterns of the shares, however, have no visual meaning and hinder the objectives of visual cryptography. Extended visual cryptography [10] was proposed recently to construct meaningful binary images as shares using hyper-graph colorings, but the visual quality is poor. In this paper, a novel technique named halftone visual cryptography is proposed to achieve visual cryptography via half-toning. Based on the blue-noise dithering principles, the proposed method utilizes the void and cluster algorithm [11] to encode a secret binary image into halftone shares (images) carrying significant visual information. The simulation shows that the visual qualities of the obtained halftone shares are observably better than that attained by any available visual cryptography method [9].

E. LSB Based Steganography using Genetic Algorithm and Visual Cryptography for Secured Data Hiding and Transmission

A large number of commercial steganographic programs use the Least Significant Bit (LSB) embedding as the method of choice for hiding data as it has low computation complexity and high embedding capacity. Although there has been an extensive research work in the past, but majority of the work has no much optimal consideration for robust security towards the encrypted image. The proposed system provides the best approach for secure data hiding and transmission over Networks using LSB based steganography with Genetic Algorithm (GA) and Visual Cryptography (VC). The system here encodes the secret message in least significant bits of the cover image so termed as stego image by using a secret key. Genetic Algorithm and Visual Cryptography has been used for enhancing the security. Genetic Algorithm is used to modify the pixel location of stego image which is another protection lock for the secret message and image and the detection of this is complex. Visual Cryptography is further used to encrypt the modified pixel image by breaking it into

two shares based on a specific threshold, later those encrypted shares and the secret key is separately sent to other. The main aim of this paper is to design the enhanced secure algorithm which uses both steganography using Genetic Algorithm and Visual Cryptography to ensure improved security and reliability [12].

IV. PROPOSED APPROACH

Visual cryptography is a unique standard of advance cryptography, which is used in a verity of applications for providing the security of data, authentication and authorization. There are various kind of visual cryptographic schemes are available, in addition of that all of them are unique in their concept. In each cryptographic approach, system uses the image for encryption and decryption. Due to study that is known this cryptographic approach is highly secured with their hidden credentials. But this technique is never used for securing text data. Thus a new data security algorithm is required to work with the text data as well as image data too.

The proposed work is an extension of the visual cryptography which is derived using the domain of traditional visual cryptography and text processing technique. The proposed methodology is works with both kinds of data for securing them text as well as image. That is processed using the following approach.

1. Text data: Text data first converted into byte format and then again, it is converted into binary format for processing. Here an image is constructed using the text for further processing of information processing.

2. Image file: In this technique the traditional technique is slightly modified with the random selection process, which is keep in track using a binary sequence of string for decryption purpose.

The overview of the proposed visual cryptographic technique is described in the given figure 2. The proposed system contains a number of different components which helps to manipulate and share the information securely in a public network.

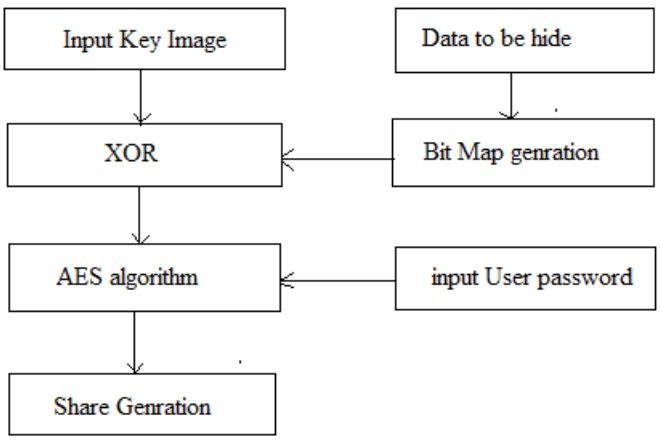

Figure 2 proposed VSS scheme

The proposed secrete sharing model is given using figure 2, in this diagram a key image is required on which the data is embedded for hiding. On the other hand the data to be hiding is produced as input to the system. System first recognizes the format of data. If the data is in format of image then simple XOR operational block is called otherwise the input text data is captured in form of bytes and then after a bit map is defined on the basis of recovered bytes. During the XOR process the key image is first decomposed on their components of [R, G, B] and using their values a binary string is formed. By using the binary string and the bit map string of data the XOR operation is performed. During the XOR process the key image binary string and outcome of the XOR operation is both the data is combined each other. The combined data is further produced with the user defined password and a cryptographic algorithm that improves the strength of generated cipher text. The outcome of this phase is again converted into a bit map and for further processing two shares of bit map is created.

In this paper the theoretical concept of data or information sharing is presented. In near future their detailed implementation is described.

V. CONCLUSION

The proposed study is initiated with the aim to find the solution for information sharing and cryptographic algorithm investigation. Thus a number of different research articles are studied and a new concept of cryptographic manner namely visual cryptography is studied. In this technique the key efforts are made to distribute the information using the shares of single information and the entire message is recovered when all the shares are combined each other. But this technique having some weakness on share generation thus a new solution for preparing the secret shares is proposed. The proposed technique not only converts the information into a number of shares that also improve their shares to be recovered only by the provided system. In near future the given technique is implemented using the JAVA technology and their performance and implementation aspects are described.

REFERENCES

[1] D Elizabeth Rob, Denning, "Cryptography and Data Security", http://faculty.nps.edu/dedennin/publications/DenningCryptographyDataSecurity.pdf
[2] Kartik Krishnan, "Computer Networks and Computer Security", Lectures 22-24, Mar 8-11 2004
[3] "Chapter 11 - Asymmetric Encryption", https://cseweb.ucsd.edu/~mihir/cse207/w-asym.pdf
[4] Sozan Abdulla, "New Visual Cryptography Algorithm For Colored Image", JOURNAL OF COMPUTING, VOLUME 2, ISSUE 4, APRIL 2010, ISSN 2151-9617
[5] Bharanivendhan N, Amitha T, "Visual Cryptography Schemes for Secret Image Sharing using GAS Algorithm", International Journal of Computer Applications (0975 – 8887) Volume 92 – No.8, April 2014
[6] ShyongJianShyu, Shih-Yu Huang, Yeuan-Kuen Lee, Ran-Zan Wang, Kun Chen, "Sharing multiple secrets in visual cryptography", 0031-3203/$30.00 2007 Pattern Recognition Society. Published by Elsevier Ltd.
[7] Bin Liu, Ralph R. Martin, Shi-Min Hu, "Structure Aware Visual Cryptography", Computer Graphics Forum c 2014 The Eurographics Association and John Wiley & Sons Ltd. Published by John Wiley & Sons Ltd.

[8] Priyanka Agrawal and Vijay Kumar Sharma, "IMPROVED ALGORITHM FOR VISUALCRYPTOGRAPHY USING REGION INCREMENTATION", SSN 2319-5991 www.ijerst.com, Vol. 3, No. 4, November 2014, © 2014 IJERST. All Rights Reserved
[9] Zhi Zhou, Gonzalo R. Arce, and Giovanni Di Crescenzo, "Halftone Visual Cryptography", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 15, NO. 8, AUGUST 2006
[10] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Extended capabilities for visual cryptography," Theoret. Comput. Sci., vol. 250, no. 1–2, pp. 134–161, 2001.
[11] R. A.Ulichney, "The void-and-cluster method for dither airay generation," in Proc. SPIE, Human Vision, Visual Processing, Digital Displays IV, Sep. 1996, vol. 1913, pp. 332–343.
[12] B. PRASAD, K.C.LAKSHMI NARAYANA, "LSB Based Steganography using Genetic Algorithm and Visual Cryptography for Secured Data Hiding and Transmission", Copyright @ 2014 SEMAR GROUPS TECHNICAL SOCIETY. All rights reserved.