

An Analysis on Visual Cryptography

¹Midhuna Murali. C, ²Manjusha. P and ³Shobana. D

^{1,2}Scholar, ³Assistant professor,

^{1,2,3}IT Department, Sri Krishna Arts and Science College, Kuniyamuthur, Coimbatore, TamilNadu, India

Abstract: Computer and network security is one of the most Crucial areas today. With so many attacks happening on all kinds of computer systems and networks, it is imperative that the subject be understood by students who are going to be the IT professionals of the future [1]. This paper includes discrete structures used in stream and block ciphers in symmetric cryptography and gives a brief description about the advantages, disadvantages and applications of visual cryptography [2].

Keywords: Encryption, Decryption, Confidentiality, Integrity, Non-repudiation, Authentication, Visual Cryptography.

I. INTRODUCTION

A. Definition

The Visual cryptography indicates the science of coding and decoding messages so as to keep these messages secure. Coding takes place using a key that ideally is known only by the sender and intended recipient of the message. [3]

B. Overview

The four objectives of Modern Cryptography are:

1. Confidentiality (the information cannot be understood by anyone for whom it was unintended)
2. Integrity (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected)
3. Non-repudiation (the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information)
4. Authentication (the sender and receiver can confirm each other's identity and the origin/destination of the information).

The word is derived from the Greek word *Kryptos*, meaning hidden. The origin of cryptography is usually dated from about 2000 BC, with the Egyptian practice of hieroglyphics. These consisted of complex pictograms,

the full meaning of which was only known to an elite few. The first known use of a modern cipher was by Julius Caesar (100 BC to 44 BC), who did not trust his messengers when communicating with his governors and officers. For this reason, he created a system in which each character in his messages was replaced by a character three positions ahead of it in the Roman alphabet.[4]

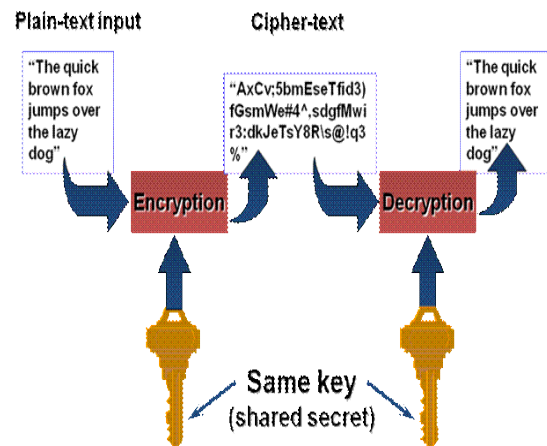


Figure 1: Encryption and Decryption [9]

II. VISUAL CRYPTOGRAPHY

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. The technique was proposed by Naor and Shamir in 1994. 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. Both transparent images and layers are required to reveal the information. The easiest way to implement Visual Cryptography is to print the two layers onto a transparent sheet [5].

A. Types of Visual Cryptography

1. Traditional Visual Cryptography.
2. Extended Visual Cryptography

3. Dynamic Visual Cryptography
4. Color Visual Cryptography
5. Progressive Visual Cryptography
6. Image Hatching for Visual Cryptography
7. Applications for Visual Cryptography.[6]

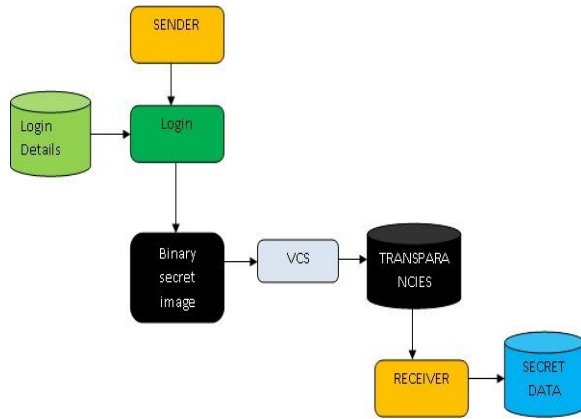


Figure 2: Logical Representation of Visual Cryptography [11]

B. Applications

- Biometric security.
- Water marking.
- Steganography.
- Printing and scanning application.
- Bank Customer Identification.
- Bank sends customer a set of keys in advance.
- Bank website displays cipher.
- Customer applies overlay, reads transaction key.[7]

C. Advantages

- Easy to implement.
- Decryption algorithm not required (Use a human visual System). So a person unknown to cryptography can decrypt the message.
- We can send cipher through fax or e-mail.
- Lower computational cost since the secret message is recognized only by human eye not cryptographically computed.[8]

D. Disadvantages

- The contrast of the reconstructed image is not maintained.
- Perfect alignment of the transparencies is troublesome.

- Its original formulation is restricted only to binary images. For colored images additional processing has to be done.[8]

CONCLUSION

- Advantages of Visual Cryptography is the scheme is the property VCS decoding relies purely on human visual system.
- Visual cryptography is used with messages, therefore giving the cryptanalyst little to work with.
- Since visual cryptography uses short messages, public keys can be encrypted using this method.
- Visual cryptography has proved that security can be attained with even simple encryption schemes.

References

- [1] Book: Cryptography and Network Security. Author: Atul Kahate.
- [2] <http://www.springer.com/computer/security+and+cryptology/journal/12095>.
- [3] <http://dictionary.reference.com/browse/cryptography>.
- [4] <http://searchsoftwarequality.techtarget.com/definition/cryptography>.
- [5].<http://users.telenet.be/d.rijmenants/en/visualcrypto.htm>.
- [6] <http://bookboon.com/en/visual-cryptography-and-its-applications-ebook>.
- [7] <http://www.slideshare.net/PratikshaPatil/visual-cryptography1>.
- [8] <http://www.slideshare.net/pallavikhandekar212/visual-cryptography-15843873>
- [9] <https://images.search.yahoo.com/images/view>
- [10] http://pages.csam.montclair.edu/~robila/SECURITY/F2005_P/P16/Visual_Cryptography.pdf
- [11].<https://images.search.yahoo.com/images/view>