Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 3, March 2015, pg.253 – 258

RESEARCH ARTICLE

Understanding Steganography over Cryptography and Various Steganography Techniques

[1]Rajesh Kumar, [2]A.J. Singh

[1,2]Computer Science Department, HPU, Shimla, India

[1] Rajeshkumar82@live.com; [2] aj.hpucs@gmail.com

***Abstract:** This paper is all about the study of the steganography and techniques used for the steganography. Firstly we will understand the term steganography, use of steganography and techniques used for the steganography. In steganography, we use text transformation, LSB (Least Significant Bit), graphics or image steganography, audio steganography, steganography in videos and animations etc. This paper includes the study of these techniques and how it works.*

***Keywords:** Steganography, Cryptography, steganography techniques, text steganography, LSB, watermarking, crossbreeding*

I. INTRODUCTION

Steganography is a technique to embed the data in the content like text, images, videos etc. by means of providing security to the data which has been sent over the internet or mail. The word steganography has its own meaning i.e. hidden writing. The word "Steganography" is formed by the two Greek words that are "Stegos means Hidden or Covered" and "Grafia means writing". The notion of data hiding or steganography was first introduced with the example of prisoners' secret message by Simmons in 1983. [**1**].

We can use steganography over the cryptography, these are very closely related to each other. The use of cryptography as a way to secure the hidden message mainly addresses the security requirement in the Information-Hiding system. For the purpose of steganography, symmetric encryption is followed. The symmetric encryption is a method of encryption that uses the same key to encrypt and decrypt a message.

If one person encrypts and decrypts data, that person must keep the key secret. If the data is transmitted between parties, each party must agree on a shared secret key and find a secure method to exchange the key. The security of encrypted data depends on the secrecy of the key.

If someone gains knowledge of the secret key, he or she can use the key to decrypt all the data that was encrypted with the key. No encryption method is completely secure. Given knowledge of the algorithm and enough time, attackers can reconstruct most encrypted data. A strong algorithm (the one that is built on sound mathematical methods, creates no predictable patterns in encrypted data, and has a sufficiently long key) can deter most attacks.[**2**.]

Cryptography scrambles messages so they cannot be understood. Steganography on the other hand, will hide the message so there is no knowledge of the existence of the message in the first place. In some situations, sending an encrypted message will arouse suspicion while an “invisible” message will not do so. Both sciences can be combined to produce better protection of the message. In this case, when the steganography fails and the message can be detected, it is still of no use as it is encrypted using cryptography techniques. There exist two types of materials in steganography: message and carrier. Message is the secret data that should be hidden and carrier is the material that takes the message in it. There are many types of steganography methods. In this paper, we are going to take a short look at different steganography methods. [1]. Fig. 1 below shows the different steganography approaches.

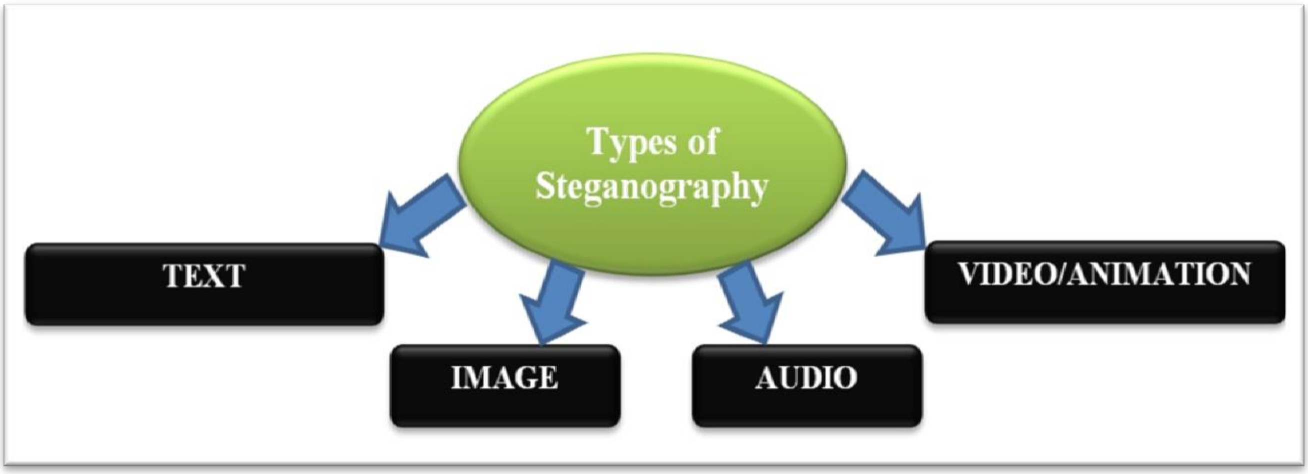

Fig. 1 Different steganography approaches.

II. STEGO-DEFINED SYSTEM

A classical steganographic system’s security relies on the encoding system’s secrecy. Although such a system might work for a time, once it is known, it is simple enough to expose the entire received media passing by to check for hidden messages ultimately, such a steganographic system fails [**2].**

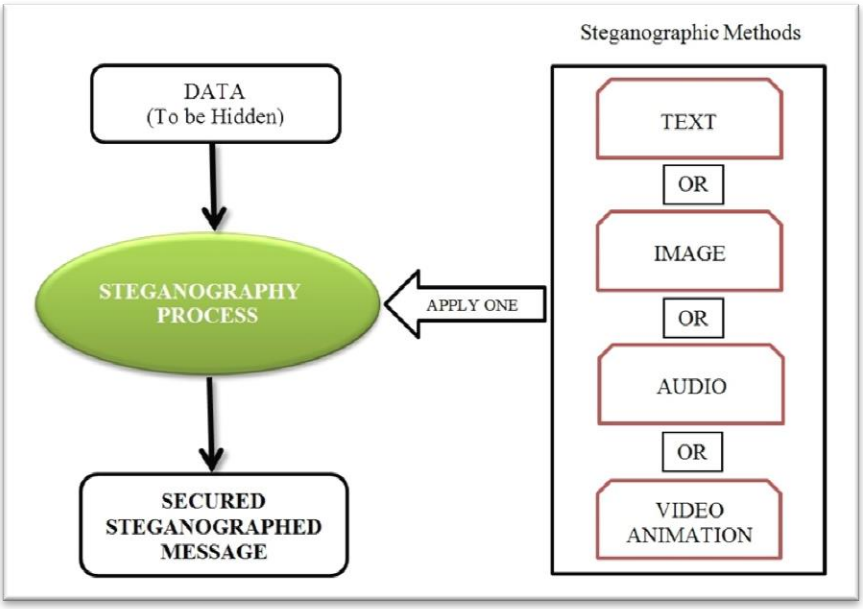

Fig. 2 Overview of Steganographic System

Though the fields of steganography and cryptography are associated with one another, there is a distinction to be made. Cryptography is the art of jumbling a message so that a would-be eavesdropper cannot interpret the message. Steganography, on the other hand, is the art of hiding a message so that a would-be eavesdropper is unaware of the message's presence. While steganography has been around for centuries, the Digital Revolution has sparked a renewed interest in the field. For instance, the mass media industry has shown increasing interest in steganography to fight piracy.

In the steganography cover media is the carrier medium – such as text, image, audio, video and even the network packet. The secret message is the private message that is to be hidden in the cover media. [3]

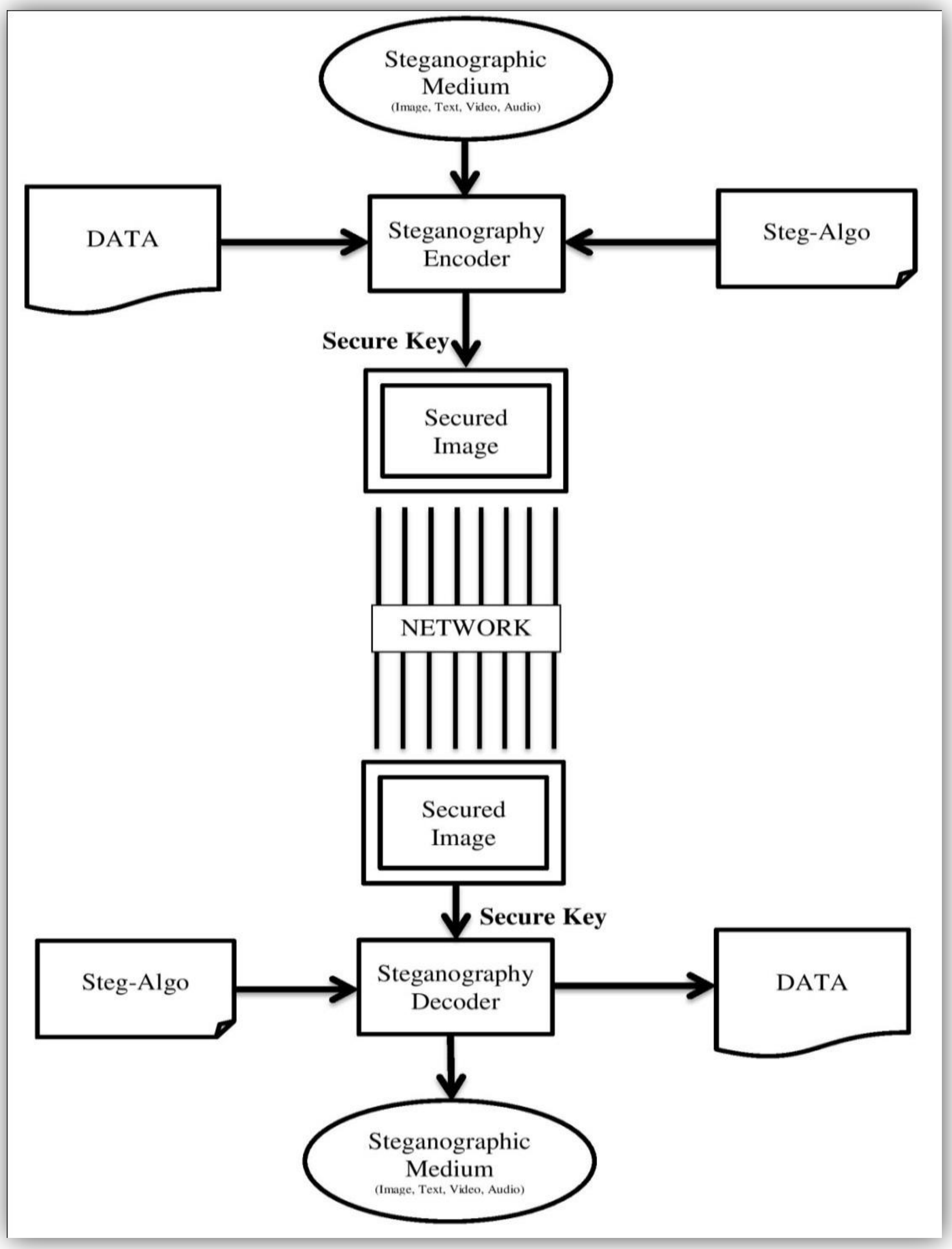

Fig. 3 Steganography process.

III. COMPARISON OF DIFFERENT STEGANOGRAPHY TECHNIQUES AND FEATURES

An information-hiding system is characterized be having three different aspects that contend with each other as: capacity, security, integrity, robustness, transparency and temper resistance etc. Capacity refers to the amount of information that can be hidden in the cover medium, security to an eavesdropper's inability to detect hidden information, and robustness to the amount of modification the steganographic medium can withstand before an adversary can destroy hidden information.

Generally speaking, information hiding relates to both watermarking and steganography. A watermarking System's primary goal is to achieve a high level of robustness-that is, it should be impossible to remove a watermark without degrading the data object's quality. Steganography, on the other hand, strives for high security and capacity, which often entails that the hidden information is fragile. Even trivial modifications to the steganographic medium can destroy it [2].

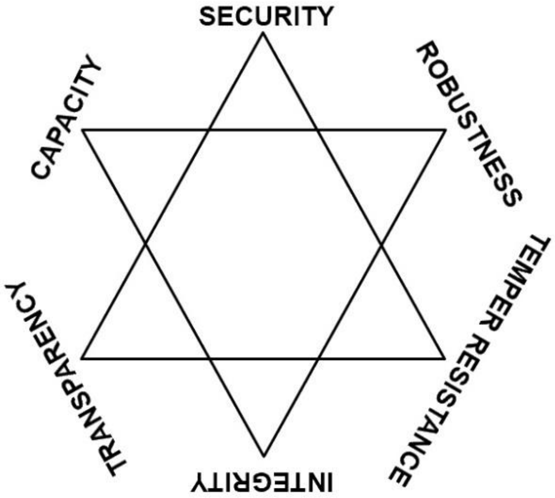

Fig. 4 Steganography features.

TABLE I
COMPARISON OF DIFFERENT STEGANOGRAPHY TECHNIQUES

Technique	**Security**	**Capacity**	**Transparency**	**Integrity**	**Temper resistance**	**Robustness**
Text Steganography	High	Low	Low	Low	High	Low
Image Steganography	High	High	Low	High	High	High
Audio Steganography	Low	Low	Low	Low	High	Low
Video Steganography	High	High	High	Low	High	Low

IV. CRYPTOGRAPHY

Computer security people often ask for non-mathematical definitions of cryptographic terms. The basic terminology is that cryptography refers to the science and art of designing ciphers; cryptanalysis to the science and art of breaking them; while cryptology, often shortened to just crypto, is the study of both. The input to an encryption process is commonly called the plaintext, and the output the ciphertext. Thereafter, things get somewhat more complicated.

There are a number of cryptographic primitives—basic building blocks, such as block ciphers, stream ciphers, and hash functions. Block ciphers may either have one key for both encryption and decryption, in which case they're called shared key (also secret key or symmetric), or have separate keys for encryption and decryption, in which case they're called public key or asymmetric. A digital signature scheme is a special type of asymmetric crypto primitive. [4].

V. AN EARLY STREAM CIPHER

An early stream cipher is commonly ascribed to the Frenchman Blaise de Vigenère, a diplomat who served King Charles IX. It works by adding a key repeatedly into the plaintext using the convention that A = 0, B = 1 , . . . , Z = 25; and addition is carried out modulo 26—that is, if the result is greater than 25, we subtract as many multiples of 26 as are needed to bring us into the range [0, . . . ,25], that is, [A, . . . ,Z]. Mathematicians write this as:

$$C = P + K \bmod 26$$

For example, when we add P(1 5) to U(20) we get 35, which we reduce to 9 by subtracting 26; 9 corresponds to J, so the encryption of P under the key U (and of U under the key P) is J. In this notation, Julius Caesar's system used a fixed key, K = D (modulo 23, as the alphabet Caesar used wrote U as V, J as I, and had no W), while Augustus Caesar's used K = C, and Vigenere used a repeating key, also known as a running key. [4]

VI. CROSSBREED (RSA +DES) ALGORITHM TO ENHANCE SECURITY FOR MULTIMEDIA CONTENT

Cloud computing is associate degree rising computing paradigm wherever computing resources like severs, network, storage and services area unit delivered as a service over a network. In cloud computing there are a unit central remote servers that maintain data and applications. Cloud Computing relies on 5 attributes as multitenancy, large quantifiability, elasticity, pay as you go, self-provisioning of resources. Cloud Computing is providing lots of benefits to its users however there's a drag of security.

The user info is keep within the cloud server and therefore the user needs that the information keep ought to be safe from unauthorized access. Third party auditor is about to handle the information to and from the cloud server to the user. Any alterations within the functioning of the third party auditor would relate to some attack by the interloper and should hurt the confidentiality of the information keep. Over this data causation and receiving from the cloud server conjointly want some security measures. Several security measures are developed to resist the safety issues in cloud computing. However still several cyber-attacks had occurred on the information storage unit and on the information communicated between the user and there the cloud server.

Although there are a unit several security problems in cloud computing the usage of cloud computing is increasing at a rapid rate. Several companies and organizations move their data to the cloud the information undergoes several changes and there are several challenges to overcome. To be effective, cloud data security depends on more than merely applying applicable data security procedures and countermeasures.

Computer based security measures largely capitalizes on user authorization and authentication. The cloud computing offers benefits to business user particularly small business user in terms of cash saving for infrastructure and software cost. [5].

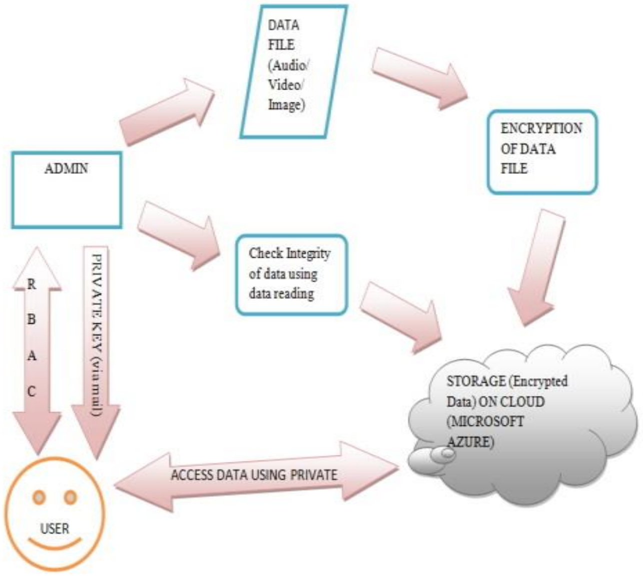
DATA FILE (Audio/ Video/ Image)
ENCRYPTION OF DATA FILE
ADMIN
Check Integrity of data using data reading
R B A C
PRIVATE KEY (via mail)
STORAGE (Encrypted Data) ON CLOUD (MICROSOFT AZURE)
ACCESS DATA USING PRIVATE
USER

Fig. 5 Crossbreed algorithm working.

VII. PROPOSED WORK

In the future work or proposed work I want to make a security application which will include the encryption methods made by crossbreeding algorithm and further output in encrypted by steganography methods will be of choice as Text Steganography, Image Steganography, Audio Steganography or Video/Animation Steganography. Steganography technique will be used randomly and the crossbreeding algorithm will also be used randomly for making the file more and more secure to send on any network. Security will be provided to make the file more encrypted and totally hidden in steganographic medium so that the data nor be extracted by another medium neither be hacked by the hackers. The working of proposed system is shown by the Fig. 6.

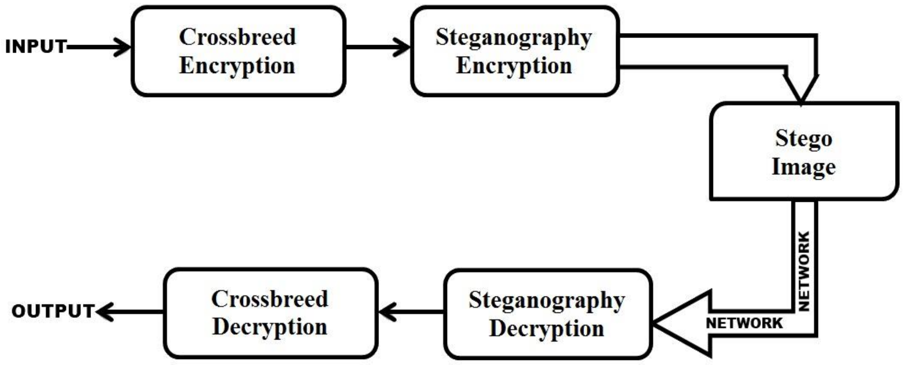

Fig. 6 Steganography using crossbreed encryption.

VIII. CONCLUSION

This research paper is all about the introduction of steganography and cryptography. This includes the study of steganography methods and techniques and how steganography works. As we know that steganography is more secure medium than cryptography. In steganography the transmitting medium is any media file such as Image, Audio, Video or animation so this is very often that nobody is bothered about the message behind the media but in case of cryptography data is in encrypted form so the hackers are more aware of it. In this research paper we talk about the technique crossbreeding algorithm used with steganography so that we can get more security to send the files even over the open networks.

ACKNOWLEDGEMENT

This work is partially supported by Computer Science department of the Himachal Pradesh University.

REFERENCES

[1] Masoud Nosrati, Ronak Karimi, Mehdi Hariri, *An introduction to steganography methods,* World Applied Programming, Vol (1), No (3), August 2011. 191-195.

[2] Ali Al-Ataby and Fawzi Al-Naima, *A Modified High Capacity Image Steganography Technique Based on Wavelet Transform,* The International Arab Journal of Information Technology, Vol. 7, No. 4, October 2010

[3] Anjali Dua, Sonia Sharma, *Design and Implementation of Steganography Algorithm using Color Transformation*, IJCSIT, Vol. 3 (4) , 2012,4692-4695

[4] G. Julius Caesar, John F. Kennedy, *Cryptography,* Security Engineering: A Guide to Building Dependable Distributed Systems.

[5] Mr.Ashish Sharma, Mr. Vikas Gupta, *Crossbreed Algorithm to enhance security for multimedia content An Overview, IJCSE*.