A Survey on various patterns regarding Encryption, a efficient based Method Regarding Cryptography and Steganography

S. B. Mahale
M.E.,Computer Sci.& Engg.
G H Raisoni IEM,
Jalgoan(NMU)

Prof. Patil Sonal
Department of Com. Sci. & Engg,
G H Raisoni IEM,
Jalgoan(NMU)

Abstract - It has been that suppose putting some data on your mail account and cloud, it necessary to the data should have secured, Data storage on the cloud is putting by the other parties. Maintaining the privacy of such data from an unauthorized user is a big concern. Circumstances-Regarding Encryption (CRE) is a promising method that addresses this concern effectively. Paper presents CRE with its most specific and complementary types. Paper compares CRE method with different parameters which helps to select best suitable method to deal with data security of an application. In this paper we deal to give higher data security using cryptography and steganography.

Keywords: Circumstances regarding encryption (CRE), cloud computing, data privacy, Cryptography, steganography, Secret sharing.

I. INTRODUCTION

In recent years in cryptography, Circumstances-regarding Encryption (CRE) has earned lots of popularity & success in the research area of cryptography [6]. CRE has two main types – CPCBE & KPCBE. Besides them, Identity-Based Encryption (IBE) is a specialized application of CBE which is used in biometrics applications. Sending a plain text of data to the receiver over a network is not secure. Confidentiality of the message is lost if the message is not protected properly. Even if the message is encoded before sending the message, it can be decoded by the hacker by making use of certain algorithm. In this paper we focus to maximize the privacy to data by providing higher security in terms of cryptography and Steganography. We are using combinations of best algorithms for to preventing in cryptography using Steganography and show that it is not cheating resistant. Encrypt the message or data which you want to send over intranet and decrypt this message using some key. This technique is called as Cryptography. Hide the data or information behind different type's images. This technique is called as Steganography.

It is the practice and study of techniques for secure communication in the presence of third parties. More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries [3] and which are related to various aspects in information security such as data confidentiality, data integrity, and authentication [4].

II. IDENTITY-BASED ENCRYPTION & ENCRYPTION BASED SYSTEMS

The scientist Sahai-Waters [5] was the first who conceived CRE. They have dealt with certain amount of error tolerance in IBE. In IBE, user is given with an identity, which is basically the string. In CRE, user is associated with set of attributes used to encrypt a message. CRE is advantageous than other encrypted schemes. It allows user to store private documents addressed to group of users fitting a specific set of requirements on public server.

III. KEY-POLICY ATTRIBUTE-BASED ENCRYPTION

There are two major categories in which existing RBE scheme can be categorized: Key-Policy RBE (KP-RBE) and Cipher text-Policy CRE (CP-CRE). Goyal, Pandey, Sahai and Waters introduced KP-RBEin [2]. Deviates from Sahai-Waters original construction which indicates that user have set of attributes and documents would be encrypted under those set of attributes. User would be able to decrypt the cipher text if cipher text attributes are within certain acceptable threshold. As mentioned earlier, after more complex structures were created, there were no ways to create AND gate which should not be susceptible to collusion attack. As security and usefulness of CRE scheme is expected, collusion resistance is must but achieving this had been considered as a critical flaw in practicality. KP-RBE and CP-RBE are complimentary schemes that both address this limitation.

IV. Ciphertext-Policy Attribute- Based Encryption

Bathencourt, Sahai & Water were the first who introduced CP-CRE in [1].It is a contrast of KP-CRE in which user have an access structure (associated with set of attributes)used for encryption, rather than encrypting a message with attributes directly. In CP-RBE, message is decrypted when user hold set of attributes and if these attributes satisfies an access policies. [1] has contributed few to RBE, where as it shows in details CPRBE toolkit which demonstrates complete implementation of CP-RBE.[1]concentrates on collision resistance scheme, and it is achieved by randomizing user's private keys. [1] also presents key revocation scheme which allows decryption of a message if user's current date key is more current than the date key that has been used to encrypt a message. Assuming this as a valid revocation scheme is little bit tedious work as it allows user to decrypt a message even after his key is expired. This is a scheme which always allows user to access a message that he had accessed once. This scheme does not allow per user access revocation.

V. Literature Survey

"A Recursive Threshold Visual Cryptography Scheme" in 2009 -Abhishek P. & Subhash K.

This paper presents a recursive hiding scheme for secret sharing [6]. In recursive hiding of secrets, the user encodes additional information about smaller secrets in the shares of a larger secret without an expansion in the size of the latter, thereby increasing the efficiency of secret sharing. An extension of secret sharing schemes is visual cryptography that aims at splitting images into two or more shares such that when a predetermined number of shares are aligned and stacked together, the secret image is revealed.

Cheating prevention in Visual Cryptography using steganography" in 2012 -by Yu Che Chan

The main goal of secret sharing is to protect important secret data, such as cryptographic keys, from being lost or destroyed without accidental exposure [7].The protection of participants is not the main concern. Since there is no restriction on the behaviour of the participants, any participant, called a cheater, can reveal a forged share on purpose.

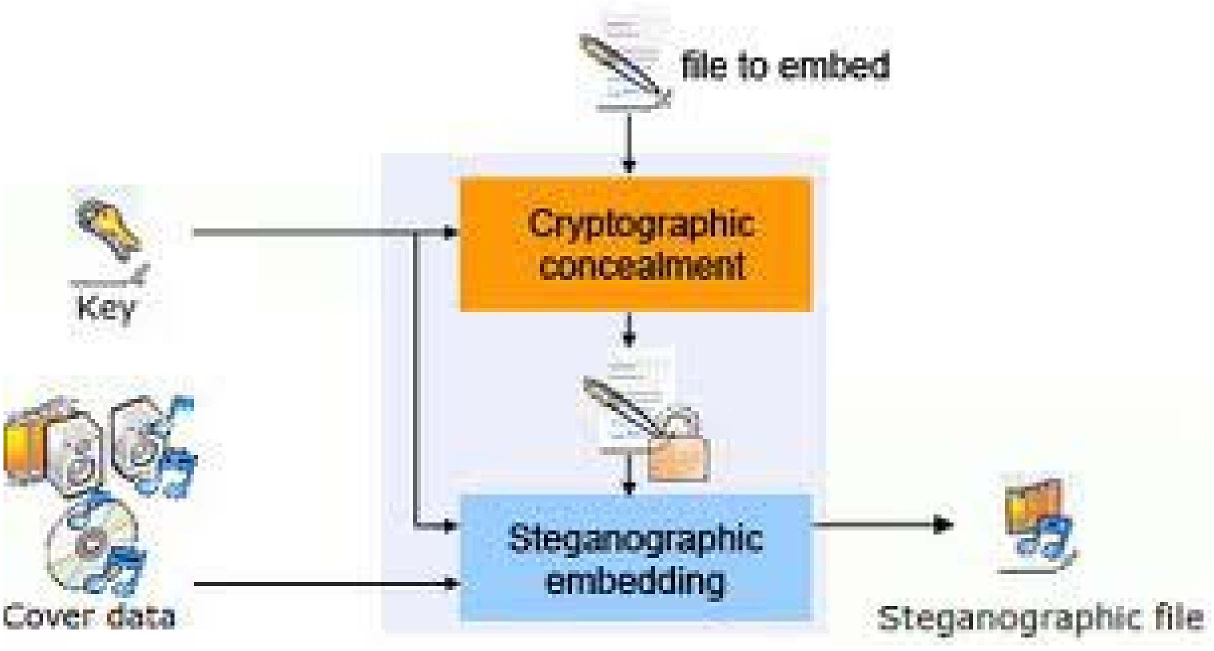

Fig: 1 Example on Cryptography Steganegraphy

Steganography is the art of hiding a secret message inside another message.

The advantages of this system is that recursive hiding of secrets was proposed with applications to both images and text, to increase the efficiency of visual cryptography and to make it possible to incorporate additional secret information that serves as a steganography channel.

The disadvantage of this system is that however, conventional approaches to visual cryptography also suffer from inefficiency in terms of number of bits of secret conveyed per bit of shares and Difficulty in getting original image.

.

Fig: 2 Example on Steganegraphy

Computer files contain unused or insignificant areas of data and also hard to detect the data behind the images. Following are the Advantages of this system: Double security is being provided within system. The hacker never finds the secret key of system as both cryptography & steganography used. It's difficult to detect data.

Sr.no	Authors	Year	Image format	Pixel Expansion
4	C.M.Hue & W.G.Tzeng	2007	Binary	Random
6	Yu-Chi Chen & Gwoboa	2012	Binary	Meaningful

Table 1: Analysis of Literature Survey

VI. CONCLUSION

CRE is useful to build encryption framework irrespective of applications. It takes care of policy enforcement and Access control in concern with cryptography and steganegraphy. Steganography to provide higher security to data, messages transmitted over transmission media such as internet. So that the paper is to studying on different authors views and to provide higher security to the data.

REFERENCES

[1] Bethencourt, A. Sahai, and B. Waters. "Ciphertext Policy Attribute-Based Encryption" In IEEE Symposium on Security and Privacy, pp. 321-334, 2007**.**

[2] V. Goyal, O. Pandey, A. Sahai, and B. Water "Attribute- Based Encryption for fine-grained access control of encrypted data", In *ACM Conference on Computer and Communications Security*, pp. 89-98, 2006.

[3] . Horne, T. H. Chen, and D. S. Tsai, "Cheating in visual cryptography,Des" Codes, Cryptog., vol. 38, no. 2, pp219– 236 Feb. 2006.

[4] M. Pirretti, P. Traynor, P. McDaniel, and B.Waters."*Secure attribute-Based Systems*", In*ACM Conference on Computer and Communications Security*, pp. 99-112, 2006..

[5] Sahai and B. Waters."Fuzzy Identity-Based Encryption", In *Eurocrypt 2005*.

[6] R. De Prisco and A. De Santis, "Cheating immune threshold visual secret sharing" Computes J.vol. 53, no 9, pp. 1485, 1496, Nov. 2009, 10.1093/ comjnl /bxp068.

[7] Yu-Chi Chen, Gwoboa Horng, and Du-Shiau Tsai, "Cheating Prevention In Visual Cryptography" Pattern Recog. Lett.vol. 23, no. 8, pp. 931–941, Jun. 2012.