International Journal of Academic Research and Development
ISSN: 2455-4197
Impact Factor: RJIF 5.22
www.academicsjournal.com
Volume 3; Issue 2; March 2018; Page No. 709-710

Review of current advent bond of cryptography and steganography

Shashi Bala
Department of Computer Science, Delhi College of Technology and Management, Delhi, India

Abstract
Digital communication witnesses an evident and continuous development in several applications on the web. Hence, a secure communication session should be provided. The protection of information transmitted across a world network has become a key issue on the network performance measures. Cryptography and steganography are two necessary techniques that are wont to give network security. In this paper, we conduct a comparative study of steganography and cryptography. We survey a variety of ways combining cryptography and steganography techniques in one system. Moreover, we present a classification of those ways and compare them in terms of the formula used for cryptography, the steganography technique and also the file kind used for covering the knowledge.

Keywords: cement emissions, environmental pollution, atmospheric changes, human health

Introduction

Information security has grown up as a major issue in our digital life. The event of recent transmission technologies forces a particular strategy of security mechanisms particularly during a state of the information communication. The importance of network security is raised day by day because the size of information being transferred across the web. Cryptography and steganography give important techniques for data security.

The most necessary motive for the offender to profit from intrusion is that the worth of the confidential information he or she will get by offensive the system. Hackers could expose the information, alter it, distort it, or use it for tougher attacks. An answer to this issue is exploitation the advantage of cryptography and steganography combined in one system.

Cryptography and steganography are two approaches accustomed secure info, either by coding the data with a key or by concealment it. Combining these two approaches in one system provides additional security. It's helpful to clarify these approaches and discuss the advantages of mixing them.

Cryptography is one amongst the standard strategies accustomed guarantee the privacy of communication between parties. This technique is that the art of secret writing, that is employed to encode the plaintext with a key into cipher text to be transferred between parties on an insecure channel. Employing a valid key, the ciphertext may be decrypted to the initial plaintext. While not the data of the key, no one will retrieve the plaintext. Cryptography plays a necessary role in several services, like: confidentiality, key exchange, authentication and non-repudiation. Cryptography provides these services for secure communication across insecure channels.

There are three kinds of cryptographic schemes for securing the data: public-key cryptography, secret key cryptography, and hash functions. These schemes are accustomed attain completely different objectives. The length and type of the keys used depend upon the type of encoding algorithmic rule.

Symmetric-key cryptography

The technique of symmetric key encoding is also called the symmetric-key, shared key and single-key encoding. During this technique, a similar secret key's used for each encoding and decoding sides. The initial data or plaintext is encrypted with a key by the sender. Then constant key's used by the receiver to decode the message and acquire the plaintext. The keys are identified solely by those two parties who are approved to do the encoding and decoding. The technique provides sensible security for transmission. However, there's a problem within the key distribution. If the key's stolen the entire information security is compromised. Moreover, a secure mechanism is required for the safe key-exchange method. Examples of symmetric-key schemes embody DES and AES algorithms.

Hash Functions

A hash function is a one-way collision-free operate with a fixed-length output. Hash functions also are known as message digests. A hash function is an algorithmic rule that doesn't use any key. However, a fixed-length hash value is calculated supported the input file such it computationally unfeasible to get the input file from the hash value, or maybe any input string that matches the given hash value. Hash functions are typically accustomed manufacture digital fingerprints of files and to ensure the integrity of the files.

Asymmetric-key cryptography

This technique is additionally called public key cryptography. It uses two keys, called public and personal keys that are mathematically associated and severally used for scripting and decrypting severally. For every user 'A', each key are required for the scheme to run. The key used for encoding is publically obtainable, thus it's known as A's public key, $Kpub_A$. There

for all alternative users will access the general public key $Kpub_A$ and encode messages to be sent to the user 'A'. On the other hand, the personal key $Kpri_A$ is just notable by the user 'A' who uses it for decoding. As a main requirement during this scheme, it's computationally unfeasible to get personal key $Kpri_A$ from the public key $Kpub_A$. An example of uneven key cryptosystem is RAC

Steganography

Steganography will be defined because the art of concealing information and communication hidden information through apparently reliable carriers in arrange to hide the existence of the information itself. So, there's no data of the existence of the message within the initial place. Steganography techniques usually use a cover, like a picture or another file, to cover the key data. If someone views the cover that the data is hidden inside, there shall be no clue that there's any hidden knowledge below the cover. During this manner, the individual will not endeavour to decrypt the information.

The secret data will be inserted into the cover media by the stego system encoder with using sure algorithmic rule. A secret message will be plaintext, an image, ciphertext, or something which may be described within the type of a bit string. When the key date is embedded within the cover object, the cover object is named a stego object. The stego object is distributed to a receiver by choosing the suitable channel, wherever a decoder system is used with a similar stego technique to extract the key data.

Benefits of combine the steganography and cryptography

It is noted that steganography or cryptography alone is meagrely for the protection of data altogether eventualities. However, if we mix these systems, we will generate additional reliable and powerful systems.

The combination of those two methods can improve the protection of the key data. This mixture can fulfil some desired options, like: memory usage, security, and strength for sensitive data transmission across an open channel. Also, it'll be a strong mechanism that permits people to speak while not dragging the attention of eavesdroppers who doesn't even understand of the existence of the key data being transmitted.

Review of literature

The significance of network security is increasing day by day because the size and sensitivity of information being transferred across the net increase. This issue pushes the researchers to do several studies to produce the required security. An answer for this issue is using the advantage of cryptography and steganography combined in one system. Several studies propose strategies to mix cryptography with steganography systems in one system. These strategies were deceased in previous surveys accessible on this subject, like revealed in 2014, that aims to provide a summary of the strategies proposed to mix cryptography with steganography systems. The authors introduced 12 strategies that are combined steganography and cryptography and created a comparative analysis. This comparative has been enforced on the premise of the necessities of security, namely: authentication, confidentiality, and strength. Another survey was published in 2014. This survey given several steganographic techniques combined with cryptography, AES algorithmic rule, Alteration component, Random Key Generation, Distortion method, Key based Security algorithmic rule.

There has been a continual rise within the number of data security threats within the recent decays. It's become a matter of concern for security specialists. Cryptography and steganography are the simplest techniques to face these threats. Today, researchers are proposing a mixed approach of each technique to attain the next level of security when each technique is used along.

Conclusion

In this paper, the concepts of cryptography, steganography and their applications within the security of digital communication across network are studied. A comprehensive technical survey of recent strategies that combined steganography and cryptography is conferred. Combining these two techniques is found to be safer than applying all of them severally.

References

1. Rajyaguru MH, Crystography-combination of cryptography and steganography with rapidly changing keys, International Journal of Emerging Technology and Advanced Engineering. 2012, ISSN, pp. 2250{2459.
2. Rahmani MKI, Kamiya Arora NP. A crypto-steganography: A survey, International Journal of Advanced Computer Science and Application. 2014; 5:149-154.
3. Seth D, Ramanathan L, Pandey A. Security enhancement: Combining cryptography and steganography, International Journal of Computer Applications. 2010. (0975{8887).
4. Abdulzahra H, Ahmad R, Noor NM. \Combining cryptography and steganography for data hiding in images, ACACOS, Applied Computational Science, 2014, pp. 978-960.
5. Khan N, Gorde KS. Data security by video steganography and cryptography techniques, 2015.
6. Kumar P, Sharma VK. Information security based on steganography & cryptography techniques: A review, International Journal. 2014, 4(10).
7. Karthik JV, Reddy BV. Authentication of secret information in image stenography, International Journal of Computer Science and Network Security (IJCSNS). 2014; 14(6):58.