IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Special Issue || Dec. 2019 || PP 39-42
International Conference on Management Practices, Innovations & Research 2019

Implementation of Video Crypto-Stegno Real Time (CSRT) System using Wang's Scheme

Ashwini rane[1], Rajesh Babu[2]
Student Mtech Computer Science Engineering, TGPCET, Nagpur
Asst.Professor Mtech Computer Science Engineering, TGPCET, Nagpur

Abstract*: Information is any sort of put away computerized data. Security is about the assurance of advantages. Information security alludes to defensive computerized protection quantifies that are applied to counteract unapproved access to PCs, individual databases and sites. Cryptography is evergreen and improvements. Cryptography ensures clients by giving usefulness to the encryption of information and verification of different clients. Pressure is the way toward diminishing the quantity of bits or bytes expected to speak to a given arrangement of information. It permits sparing more information. Cryptography is a well known methods for sending imperative data in a mystery way. There are numerous cryptographic procedures accessible and among them AES is one of the most dominant systems. The situation of present day of data security framework incorporates secrecy, legitimacy, honesty, non-renouncement. The security of correspondence is an essential issue on World Wide Web. It is about privacy, honesty, verification during access or altering of classified inside records.*

Keywords: *Data Encryption and decryption, Compression, Cryptography Concept, Security, Integrity.*

I. Introduction

To verify the information, pressure is utilized in light of the fact that it utilize less plate space (sets aside cash), more information can be move through web. It increment speed of information move from plate to memory. Security objectives for information security are Confidential, Authentication, Integrity, and Non-denial. Information security conveys information insurance crosswise over big business. Data security is a developing issue among IT associations everything being equal. To handle this developing concern, increasingly more IT firms are moving towards cryptography to secure their important data. Notwithstanding above worries over verifying put away information, IT associations are likewise confronting difficulties with ever-increasing expenses of capacity required to ensure that there is sufficient stockpiling ability to meet the association's present and future requests. Information pressure is known for diminishing stockpiling and correspondence costs. It includes changing information of a given configuration, called source message to information of a littler estimated group called code word. Information encryption is known for shielding data from listening stealthily. It changes information of a given arrangement, called plaintext, to another organization, called figure content, utilizing an encryption key. Right now pressure and encryption techniques are done independently. Cryptography before the cutting edge age was successfully synonymous with encryption, the transformation of data from a discernible state to evident garbage. Current cryptography is intensely founded on scientific hypothesis and software engineering practice; cryptographic calculations are planned around computational hardness suspicions, making such calculations difficult to break by and by any enemy. It is hypothetically conceivable to break such a framework, yet it is infeasible to do as such by any known functional methods. The development of cryptographic innovation has raised various lawful issues in the data age.

II. Cryptography

The craft of cryptography is viewed as conceived alongside the specialty of composing. As civic establishments developed, people got sorted out in clans, gatherings, and realms. This prompted the development of thoughts, for example, control, fights, matchless quality, and governmental issues. These thoughts further powered the characteristic need of individuals to discuss furtively with particular beneficiary which thus guaranteed the ceaseless development of cryptography too. The underlying foundations of cryptography are found in Roman and Egyptian human advancements.

The significance of data and correspondence frameworks for society and the worldwide economy is escalating with the expanding worth and amount of information that is transmitted and put away on those frameworks. Simultaneously those frameworks and information are likewise progressively powerless against an assortment of dangers, for example, unapproved access and use, misappropriation, change, and pulverization.

The covering up of data is called encryption, and when the data is unhidden, it is called unscrambling. A figure is utilized to achieve the encryption and unscrambling. Merriam-Webster's Collegiate Dictionary characterizes

figure as ―a strategy for changing a book so as to hide its meaning.‖ The data that is being covered up is called plaintext; when it has been scrambled, it is called ciphertext.
To shroud any information two systems are primarily utilized one is Cryptography other is Steganography. In this paper we use Cryptography. Cryptography is the study of securing information, which gives strategies for changing over information into incoherent structure, with the goal that Valid User can get to Information at the Destination. Cryptography is the study of utilizing arithmetic to encode and unscramble information.

Basic Terminology of Cryptography

Computers are used by millions of people for many purposes. such as banking, shopping, military, student records, etc.. Privacy is a critical issue in many of these applications, how are we need to make sure that an unauthorized parties cannot read or modify messages.

Cryptography is the transformation of readable and understandable data into a form which cannot be understood in order to secure data. cryptography refers exactly to the methodology of concealing the content of messages, the word cryptography comes from the Greek word "Kryptos", that means hidden, and "graphikos" which means writing.

The information that we need to hide, is called plaintext , It's the original text, It could be in a form of characters, numerical data, executable programs, pictures, or any other kind of information, The plaintext for example is the sending of a message in the sender before encryption, or it is the text at the receiver after decryption.

The data that will be transmitted is called cipher text , it's a term refers to the string of "meaningless" data, or unclear text that nobody must understand, except the recipients. it is the data that will be transmitted Exactly through network, Many algorithms are used to transform plaintext into cipher text.

Cipher is the algorithm that is used to transform plaintext to cipher text, This method is called encryption, in other words, it's a mechanism of converting readable and understandable data into "meaningless" data.

The Key is an input to the encryption algorithm, and this value must be independent of the plaintext, This input is used to transform the plaintext into cipher text, so different keys will yield different cipher text, In the decipher side, the inverse of the key will be used inside the algorithm instead of the key.

Computer security it's a generic term for a collection of tools designed to protect any data from hackers, theft, corruption, or natural disaster while allowing these data to be available to the users at the same time. The example of these tools is the antivirus program.

Network security refers to any activity designed to protect the usability, integrity, reliability, and safety of data during their transmission on a network, Network security deals with hardware and software. The activity can be one of the following anti-virus and anti-spyware, firewall, Intrusion prevention systems, and Virtual Private Networks.

Internet Security is measures and procedures used to protect data during their transmission over a collection of interconnected networks, while information security is about how to prevent attacks, and to detect attacks on information-based systems.

Cryptography Goals

By using cryptography many goals can be achieved, These goals can be either all achieved at the same time in one application, or only one of them.

These goals are:

1. **Confidentiality:** it is the most important goal, that ensures that nobody can understand the received message except the one who has the decipher key.
2. **Authentication:** it is the process of proving the identity, that assures the communicating entity is the one that it claimed to be. This means that the user or the system can prove their own identities to other parties who don't have personal knowledge of their identities.
3. **Data Integrity:** its ensures that the received message has not been changed in any way from its original form. The data may get modified by an unauthorized entity intentionally or accidently. Integrity service confirms that whether data is intact or not since it was last created, transmitted, or stored by an authorized user. This can be achieved by using hashing at both sides the sender and the recipient in order to create a unique message digest and compare it with the one that received.
4. **Non-Repudiation:** it is mechanism used to prove that the sender really sent this message, and the message was received by the specified party, so the recipient cannot claim that the message was not sent. For example, once an order is placed electronically, a purchaser cannot deny the purchase order, if non-repudiation service was enabled in this transaction.
5. **Access Control:** it is the process of preventing an unauthorized use of resources. This goal controls who

can have access to the resources, If one can access, under which restrictions and conditions the access can be occurred, and what is the permission level of a given access.

Data Encryption

A data encryption is a random string of bits created explicitly for scrambling and unscrambling data. Data encryption is designed with algorithms intended to ensure that every key is unpredictable and unique.

Cryptography uses two types of keys: symmetric and asymmetric. Symmetric keys have been around the longest; they utilize a single key for both the encryption and decryption of the ciphertext. This type of key is called a secret key. Secret-key ciphers generally fall into one of two categories: stream ciphers or block ciphers. A block cipher applies a private key and algorithm to a block of data simultaneously, whereas a stream cipher applies the key and algorithm one bit at a time.

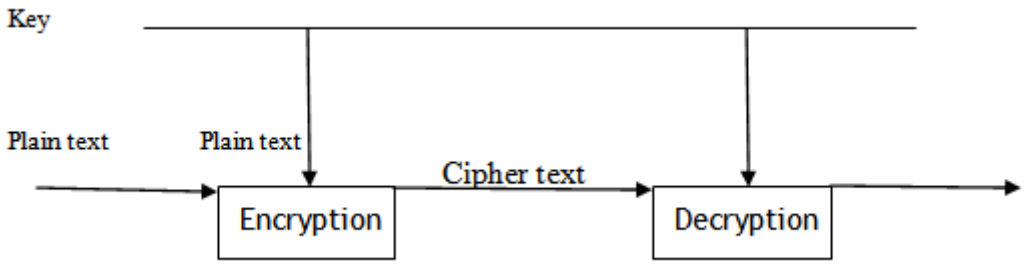
Most cryptographic processes use symmetric encryption to encrypt data transmissions but use asymmetric encryption to encrypt and exchange the secret key. Symmetric encryption, also known as private key encryption, uses the same private key for both encryption and decryption. The risk in this system is that if either party loses the key or the key is intercepted, the system is broken and messages cannot be exchanged securely.

Data Decryption

One of the foremost reasons for implementing an encryption-decryption system is privacy. As information travels over the World Wide Web, it becomes subject to access from unauthorized individuals or organizations. Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of un-encrypting the data manually or with un-encrypting the data using the proper codes or keys. Encryption is the process of translating plain text data (plaintext) into something that appears to be random and meaningless (ciphertext). Decryption is the process of converting ciphertext back to plaintext.

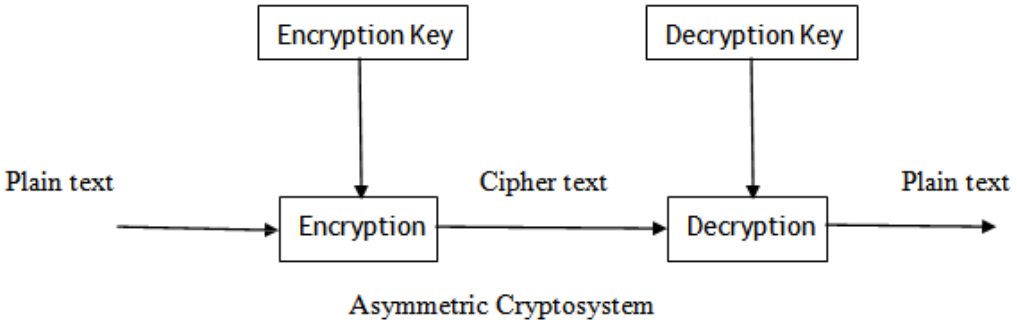
Symmetric Key Cryptography

In symmetric key cryptography is also known as private-key cryptography, a secret key may be held by one person or exchanged between the sender and the receiver of a message. If private key cryptography is used to send secret messages between two parties, both the sender and receiver must have a copy of the secret key.



Asymmetric Key CryptographySymmetric Cryptosystem

In the two-key system is also known as the public key system, one key encrypts the information and another, mathematically related key decrypts it. The computer sending an encrypted message uses a chosen private key that is never shared and so is known only to the sender. If a sending computer first encrypts the message with the intended receiver's public key and again with the sender's secret, private key, then the receiving computer may decrypt the message, first using its secret key and then the sender's public key. Using this public-key cryptographic method, the sender and receiver are able to authenticate one another as well as protect the secrecy of the message.



III. Compression

Data compression offers an attractive approach for reducing communication costs by using available bandwidth effectively. Compression algorithms reduce the redundancy in data representation to decrease the storage required for that data. Over the last decade there has been an unprecedented explosion in the amount of digital data transmitted via the Internet, representing text, images, video, sound, computer programs etc.

Data compression implies sending or storing a smaller number of bits. Compression is the reduction in size of data in order to save space or transmission time. Many methods are used for this purpose, in general these methods can be divided into two broad categories: Lossy and Lossless methods. Lossy Compression generally used for compress an images. In this original data is not identical to compressed data that means there is some loss e.g. Block Truncation Coding, Transform Coding, etc... Lossless Compression used for compress any textual data.

IV. Summary

Cryptography is used to ensure that the contents of a message are confidentiality transmitted and would not be altered. Confidentiality means nobody can understand the received message except the one that has the decipher key, and "data cannot be changed" means the original information would not be changed or modified.

References

[1]. Swarnalata Bollavarapu and Ruchita Sharma-– Data Security using Compression and Cryptography Techniques|
[2]. Manoj Patil, Prof. Vinay Sahu—– A Survey of Compression and Encryption Techniques for SMS|
[3]. Bobby Jasuja and Abhishek Pandya —– Crypto-Compression System: An Integrated Approach using Stream Cipher Cryptography and Entropy Encoding|
[4]. https://msdn.microsoft.com/en-us/library/windows/desktop/aa381939(v=vs.85).aspx
[5]. https://www.techopedia.com/definition/1773/decryption [6]www.computerhope.com/jargon/d/decrypti.htm
[6]. https://en.wikipedia.org/wiki/Cryptography
[7]. https://www.techopedia.com/definition/25403/encryption-key
[8]. http://searchsecurity.techtarget.com/definition/private-key
[9].]https://www.tutorialspoint.com/cryptography/cryptography_tutorial.pdf