International Innovative Research Journal of Engineering and Technology
Vol. 6, Issue. 3, March 2021, pp. 22~32
ISSN: 2456-1983, DOI: 10.32595/iirjet.org/v6i3.2021.145

High Data Security Using Asymmetric Key Cryptography and Linguistic Method Steganography

Shravankumar Venumula[1], Senthil Ramadoss[2]
[1]Department of Electrical and Electronics Engineering, University of Technology and Applied Sciences, Oman
[2]Department of Soft Computing, University of Technology and Applied Sciences, Oman

Article Info

Article history:

Received Dec 30, 2020
Revised Feb 20, 2021
Accepted March 17, 2021

Keywords:

Cryptography
Steganography
Asymmetric key
Tradeoff
Least Significant Bit.

ABSTRACT

This paper recommended response is to receive encrypted sensitive text data on personal data electronics that take control of the combination of both procedures: Steganography and cryptography. The security of the system is provided through the contribution of video-based asymmetric key cryptography followed by two sequential layers of steganography to insure security also with the best positive effects out of the latter. The experiment modeled the method and simulated it. It was developed to be studied to analyze the relationship. Between protection, skill, and concentration on data. The studies require data retention checking apps of 10 various widths showing fun video effects. The report provides capacity changes with protection, as an undesirable tradeoff enforced. The uniqueness of the work is presented in the showcase of different measures that make it hard for the service provider and the application to choose the maker of the decision. The tests given are all 1-LSB privacy awareness possibilities, 2-LSB and 3-LSB methods that detail their video interaction on the cover. The core results demonstrate to be the applicability of the 3-LSB method to be enacted offers good adequate safeguards with realistic skill preferred to win 3-LSB for 1-LSB and 2-LSB techniques.

Corresponding Author:

Shravankumar Venumula,
Department of Electrical and Electronics Engineering,
University of Technology and Applied Sciences, Oman.

1. INTRODUCTION

The investigation of secret writing is cryptography. A cipher is a concealed writing method that translates plaintext (or cleartext) into ciphertext. Encipherment or encryption is the process that transforms plaintext into ciphertext; the reverse process of transforming transcribing or decrypting is referring to as ciphertext into plaintext. Encipherment of both a cryptographic key or keys governs decipherment and decipherment. Four complimentary types of encryption methods exist transpositions and substitutions. In the details, traversability rearranges bits or characters. With a "rail-fence" for particular, the letters of a plaintext message are written down in a cipher, linked to a rail fence form, and then removed by rows. The following table shows this series. The key to the protocol is given by the fence depth, which is 3 in this case. New battery decryption replaces character bits, characters, or character blocks with the survivors. A simple form of replacements encrypts moves each letter in the French language.

Alphabet forward with K positions (shifts back to A after the Z cycle); K is the key to the Chiffre. Cipher. Usually, the transposition is contrasted with substitution in computer applications. For example, 64-bit blocks are stored and transmitted by the Data Encryption Standard (DES), using a transposition and substitution combination. The investigation of methods of destroying encryption methods is cryptanalysis. If the plaintext or key can be estimated from the ciphertext, or if the key can even be determined from plaintext-

ciphertext pairs, the cryptosystem is breakable. Three are basic attack methods: ciphertext-only, known-plaintext, and specified.

Usually need to protect the privacy Which Store messages via e-mail, health records, family private documents, credit card details, and credit on personal computers info on cards. Securing hidden valuable texts the privileges of personal computers (PCs) are the ability to allow eligible files from the PC to respond as a private cover[1]. With a focus on providing the user's confidence and wellbeing to protect, combine cryptography with expertise on a PC technique of steganography, i.e. the hiding of data through sensitive techniques, as commonly presented for image hiding [2] but here and using steganography based on photo.

The Safeguard attained for trying to hide using steganography. Sensitive data within this cover media rests on the cover media Belief that no one would accuse Shielded of any activity. However if anyone notices that personal data appears, the cover media will be removed, to be discovered [3]. It is desired, therefore to use another encrypted data technique, such as cryptography, before obscuring the mainstream sensitive data in the cover. This maintains that no one can recognize its content because it is encrypted, even when the embedded text is announced. We should then take advantage of the fusion of the two approaches for stronger assuring that except for the very difficult security penetration; sensitive information is still sensitive; it is not hindered or negatively used [4].

Steganography (STEGə-NOG-rə-fee) a file, message, object, or video may be lodged within another file, message, image, or video. The term steganography is originated from the French steganographic, which combines the phrases steganós, meaning "covered or secret," and -graphic, meaning "writing," meaning "writing" [5]. In 1499, Johannes Trithemius steganography, a treatise on cryptography and steganography, disguised as a book on science by his, the first recorded use of the term was. Commonly, the opaque symptom to be (or to be part of something else: photos, stories, shopping lists, or some other cover text. For instance, the substitution cipher can be in invisible ink between the visible lines of a private letter. Forms of authentication through obscurity are some steganographic implementations that lack a piece of universal information, and key-dependent steganographic schemes aspire to the requirement of either Kerckhoffs [6].

The strength of the intended encryption method of steganography over cryptography alone is that a sample of the research does not refer to itself. In countries where encryption is illegal, detectable encrypted texts, independent of How unbreakable they are, can be incriminating in itself to arouse interest [7]. The operation of hiding the content of a message alone, both the fact that an encryption key is sent and its content is covered by steganography, is thus cryptography. A sender would start with a peaceful image file, for instance, and change the shape of every other hundredth pixel in the alphabet to match a letter. Latest update so subtle that the modification is likely to be lost by those who are not constantly seeking it. Privacy laws mean to protect digital information from the wrong forces and harmful acts by malicious access, such as hacking attacks or phishing scams, such as those in a database. Types of cryptography are shown in below figure 1.

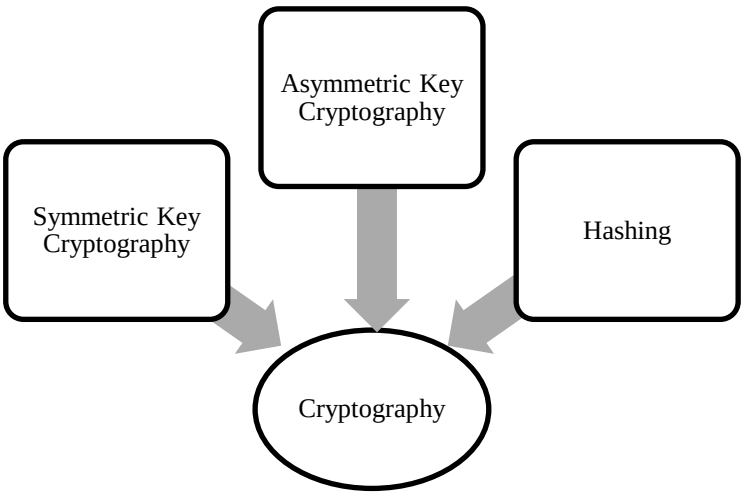

Figure 1. Types of cryptography

Asymmetric keys are the cornerstone of a cryptographic group formed Public Key Infrastructure (PKI) that contains two distinct keys, one to lock or encrypt plain text, and one to unlock or decrypt the ciphertext. Neither key will perform those functions. One key (public key) is revealed and the other key is kept secret (private key). The program enables personal communications from the public to the owner of the

unlocking key, if the lock/encryption key is the one issued. The system can help as a signature verifier of documents locked by the owner of the private key if the unlock/decryption key is the one leaked[7].

Both coordinating parties i.e. both Alice and Bob) have two keys of their own in asymmetric (public key) cryptography. Just to be sure, that's four total keys. Each entity has a public key of its own that it provides with the world and a private key of its own that they, well, which of course, they keep private, but more than what they keep as a heavily protected secret. The magic of public-key cryptography is that only with the private key should a message encrypted with the public key be decrypted. Alice is supposed to encrypt her message with the public key of Bob, and even though Eve knows that she used the public key of Bob, and even though Eve knows the public key of Bob herself, she also could not decrypt the message. Only Bob can be using his key to decrypt the message.

Since the advancement in technology is one of the most essential aspects of data creation and data correspondence has been impressive stability. Has been cryptography as a tactic to protect the mystery of correspondence, a large array of systems were developed to secure the mystery of communications. To preserve the document, encode and unscramble information mystery. Regrettably, maintaining the nature of a message mystery is often sufficient, and it may also be essential to keep the appearance of the mystery of the message. The technique used for doing just that is called steganography.

The evaluation and learning of imperceptible correspondence are shrouded by steganography. Therefore, this is the strength to impede the existence of the imparted data by concealing data in other data. There is a fine record of characterization and routine of data deception. The greeks If possible, respectable adults should correspond with their child in histories where they used to shave the head of one of their trustworthy men, far from the regulations. The message was stenciled until the skin of the head and the delivery person is shaved afterward He will once again let it be his hair. If the hair has grown back to the message, the emissary withdrawal to the statutory infant is entirely established. Then the child in law may shave the child in law. To recovered The phone, the head of the errand agent for one more time again. Steganography is a secured investigation of composition. On the first day that it was used to send signals from client to server, steganography was studied in journals. The use of undetectable, acidic powders was one such mode of steganography. This ink is undetectable, down close to the tab. If the paper on which it is written maintains light at a certain edge, the message that this ink is made of might have been read. First, with the imperceptible ink, the discharge message was prepared and now to make the additional, the letter compels either message in the con- defined time interval duration was formed in agreement.

So this was steganography in its previous phase. Steganography viably shrouds the post but does not obscure the complications imparted by board sessions. Steganography is a device that disguises the evidence or detail of discharge included in ordinary data or data. The common message used to shroud the identification of the discharge is called a transporter. The mystery message is inserted to frame the medium in the transporter for steganography. The steganographic key to encrypt and decrypt only to the sender and bene, this key will know beneficiary. At the point where an illustration is used to hide info, then the mystery documents are complete in the following case It is pointed to as steganalysis. The functionality containing the secret information is also known as watermarked when information is covered in the application. It is best to adhere to the operation as after The below figure 2. shows the flow chart of steganography

Steganographic medium = hidden information + cover-medium + steganography key.

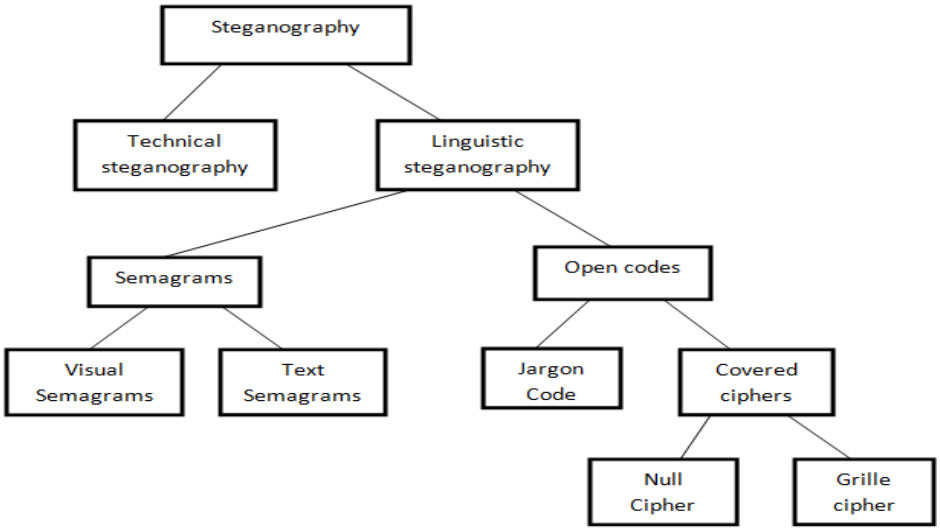

Figure 2. Steganography flowchart (8)

Steganography and cryptography are also sought in an advanced country to protect data from extreme gatherings. Steganography and cryptography both admire information, however, no innovation alone protects information. Nearly perfect and both can be conked out. Thus it is that most professionals would consider including both as a part, more levels of security are included. Steganographic advancement is an amazingly big component Plausible and monitored Internet privacy with distinction to open internet security frameworks, such as the internet. Steganographic manifestations To support the cryptography and expand the ruptures or holes or security cryptography holes. The centers of steganography to send total security. The researchers have ruined their analysts with their studies that have inhibited the routines and multi-sided efficiency of the routines by most of the legislatures encryption. The routines increased with these impediments. The builders are partially powerless. Such powerless ones the security openings are defined by rationales that if assaulted shrouded data can be easily unveiled. As a result, steganography is a solution to the concealment of protection openings and steganography is indeed always steganography. Utilizing improvements in cryptography[8].

2. RELATED WORKS

The author Ogiela, U., & Ogiela, L [9] explained that the publication provides algorithms to mitigate risk regarding unauthorized access to it. Data splitting and sharing algorithms that can learn communication to take place within a school state of secret trustees play a special place of algorithms for cybersecurity**.** This article addresses protocols of the kind outlined above and also proposes a way to use the linguistic knowledge sharing solutions proposed. With some reasonable semantic, linguistic message-sharing algorithms are categorized as a class of data retention protocols. This is because semantic analysis stimulates the knowledge of many data samples based on content. From multiple points of view, the proposed methods are very useful. The authors would like to present one useful utility for cloud computing, cognitive service management, and applications for data sharing.

The author Hamzah, A, et al.., [10] explained that linguistic steganography, descriptions of languages are used to disguise data. The Arabic language has a great selection of characteristics that have not been used in this context until now. In particular, Arabic calligraphy involves multiple fonts in different areas and Arabic alphabet letters. This paper proposes a scheme is proposed Arabic calligraphy contains necessary details. The processing, embedding period, and extraction phase are the forms of preparation phases of the framework. The embedding growing strength string matching according to a deeper meaning to derive stego text and eiq shapes. Corpus creation and a modification of the Aho-Corasick string-matching algorithm are included in the structure. Naskh, the Arabic font, as a case study, was used. A selection of Arabic poetry and proverbs were used as a dataset. Availability and protection have been assessed under the system. In every stego-system the visual difference between the cover and the stego-cover must be unnoticeable to the subject, the freedom in this mechanism is satisfying there is no cover used. The cover reinforces the deeper data itself and also provides high data embedding power. The appraisal expressed a willingness to use the various shapes of Arabic letters to fit the criteria of steganography.

The author Xiang, L., Wu, W., Li, X., & Yang, C[11] described that, though compression of secret message and preference of candidate text, novel linguistic steganography with high imperceptibility and un-detectability is recommended. The proposed word indexing compression algorithm (WIC) can eliminate the length of the practicable embedded payload, whereas its stego text selection strategy can choose the stego text with high un detectability from the candidates. By the WIC algorithm losslessly compresses the cryptic information by imposing a minimum-maximum weight algorithm with Huffman coding with the encouragement of the candidate cover text. Ten cover texts are taken from a huge cover with slight compression ratios with respect to the purpose to bolster the anti-steganalysis capacity, and the corresponding compressed secret key is embedded using synonym substitutions. A particular only one Stego text is specified by the law derived from the distance between the cover text and its Stego text. Findings further suggest that because of greater embedding productivity, the proposed compression algorithm achieves better compression ratios than Huffman and LZW coding algorithms, and our steganography performs well with compression and stego text selection rule compression anti-steganalysis capability.

The author Xiang, L, et al..,[12] explained that the integration of steganography risks the safeguards of smart campus privacy specifics. In place to avert privacy disclosure, a linguistic steganalysis procedure based on word embedding is proposed to detect user information concealed in synonyms in texts. As word embeddings, each synonym and languages in its range are represented with the continuous Skipgram language model, The above attempts to encode semantic phrases into dense vectors that become low-dimensional. Context quality, delineated by its take a keen with context features, illustrates a synonym's suitability and is effectively estimated by its corresponding word embeddings and weighted by the context words' TF-IDF values. For steganalysis, three features are extracted and fed into a support vector machine classifier tasks by measuring the differences in backdrop fitness values of synonyms in the same synonym range and the differences of those in the cover and stego text. The experimental results illustrate that the

proposed steganalysis strengthens the average F-value over two baselines by at least 4.8 percent. Therefore by acquiring better word embeddings, the intervention is required can be further intensified.

The author Taha, M. S., et al.., [13] explained that the establishment of a network is usually an indication of attacks and other sudden transformations during active communication over an unsecured network safe communication between two communicating parties became a complex question. However, either cryptography or steganography would be used to ensure the safety and security of classified material. Steganography refers to the act of concealing a message (with no traceability) in a way that makes no sense to anyone else except for the original purchaser, when cryptography refers, on the other hand, to the art of translating plaintext (message) into an unreadable format. Steganography thus wraps the essence of a deep motive, while the format of the message itself is altered by cryptography. Both steganographic and cryptographic procedures are stable. These particular thesis aims are to analyze the various ways to utilize steganographic and cryptographic methods of achieving a heuristic algorithm. In reality, some of the similarities also are presented between cryptographic and steganographic techniques.

The author Zhou, T., Shen, J., Li, X., Wang, C., & Shen, J[14] described that in every corner of the globe, cyberspace has become the most common information exchange carrier, which is beneficial to our lives in almost everything way. Cyberspace safety shortly has become the most significant commitment for the internet with the continuous expansion of the internet, especially Dewey decimal classification. They dwell on analyzing the characteristics of quantum cryptography and discussing the potential Internet gains of it. It is worth noting that in the noise-free channel, we review the quantum key distribution (QKD) protocol. In turn, we also aim for the QKD protocol in the noisy channel to simulate social reality in the future Internet. The authors found the theoretically in the future, unconditional security of quantum cryptography, ideal for the Internet as ever important impacts, is probable.

The author More, S., et al.., [15] explained that the main control at the edge and in the network blends multi-layers of security. Policies and controls become oriented across each network security layer. Network resources are accessed by access, but performers who are malicious are discouraged from completing exploits. The e-commerce industry is seeing a rapid segment that is expected to grow in recent months. With the increasingly large prominence of shopping online, major anxieties for consumers, retailers, and banks are obviously for CNP (Card Not Present), debit or credit card fraud, but also identifying information, privacy. This method creates a game plan to present only the data required in this way for the transfer of funds during online shopping, the security of user data, and the leads to improved customer satisfaction and the protection of identity theft. Proposed a credit card for online shopping by implementing text-based steganography, visual cryptography, and OTPP (One Time Password). It gives security for customer information and avoids exploitation of information about customer information. The model avoids the expense of identity fraud and preserves the preservation of customer data. Trying to minimize the interchange of data between customers and retail outlets and encouraging productive finance the technique employs the combined application of steganography and visual cryptography to switch from the shared database to the merchant account, thereby safeguarding consumer information and removing misuse of information on the merchant side.

The author Chakraborty, S, et al.., [16] explained that steganography is the review of construction methods (ecosystems) that encrypt details in a way that would be an innocuous message sent by the provided datagram between two endpoints. Steganography aims to provide authentication by making it harder to confirm adverse endpoints to prove that any private image is embedded in a given message. Almost all ecosystems operate by embedding the message to be transmitted to a cover medium and the resulting datagram, which distances from a given trivial cover by less than a targeted threshold value, is then sent over an insecure channel. Stereoscopic media was being used as a cover supplier by most sensible ecosystems so far, but few have used natural language texts as a cover medium (such as English texts). Similar ecosystems use natural language as a cover medium and consider a new approach to the building of such a device in this article

The author Bache, F, et al..,[17] explained that in side-channel use of powerful adversarial strategies against cryptographic devices and meet of the ever attack surface in today's world of digitalization and the Internet of things. While the use of side-channel countermeasures such as masking was already increasingly demonstrated experimentally, common these days, when implementing these in the mobile device, great care must be taken. There are two reasons for this the models on which these countermeasures are built do not capture the full physical reality and compliance with the requirements of the countermeasures is non-trivial in complex implementations. Therefore, validating the SCA-security of individual cryptographic application instantiations using measurements on the current phone is imperative. Implement a side-channel assessment tool in this article that mixes an efficient process based on confidence intervals, data acquisition with state-of-the-art leakage measurement. Our framework helps a sound assessment of the probable responsiveness of cryptographic implementations to side-channel attacks and is reliable against noise in the evaluation

framework. By applying them to the efficient implementation of AES, discuss the steps in the risk assessment.

3. PROPOSED WORK

Asymmetric cryptography is a technique that uses a pair of related keys to encrypt and decrypt a message and encrypt it from access control or even using one public key and one private key. Asymmetric cryptography is sometimes known as public-key cryptography. A public key is an authorization key that is used to encrypt a message by any person so that it can only be read with their private key by the intended recipient. A private key, also known as a secured key, is only more commonly linked with the key initiator. Whenever anyone pulls the public key of the intended recipient from a public directory, they can choose to send an encrypted message and use that to encrypt the message when sending it. The data user will then use their private keys key to decrypt the message. In the other direction, if the dapper its private key to encrypt the message, then the message can only be decrypted using the public key of that sender, hence sender authorization. That very encryption and decryption processes happen automatically; users will not have to explicitly enable and disable the message. HTTPS is made possible by many protocols, including Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols, which rely on asymmetric cryptography. In software items, such as browsers, which need to create a clear interaction over a dangerous network such as the internet or need to validate a digital signature, the block cipher is always used. better information security is the big benefit of asymmetric cryptography. It is the most robust form of encryption although users are never supposed to file or exchange their private keys, avoiding the risk that a cybercriminal might discover a user's private key during transmission.

For encryption and decryption, asymmetric encryption uses a mathematically compatible pair of keys: a public key and a private key. Whether either public key is used for encryption, it is also used to decrypt the connected private key; then it is used to encrypt the private key, it is used to decrypt the equivalent public key. The server and the client are the two people in the asymmetric encryption workflow, each with a pair of public and private keys over their own. The sender will procure the public key for the purchaser next week. Next, the plaintext is encrypted by the sender using the participant's public key or frequent, readable text; the ciphertext helps to make. The ciphertext is then sent to the creator, who decentralizes the ciphertext through their private key and returns it to the plaintext that is still legible. Because of the one-way nature of encryption, one sender is unable to read the messages of another sender system, even if each has the receiver's public key.

Public-key cryptography is a cryptographic scheme that uses pairs of keys: public keys that can be widely disseminated and private keys are known only to the holder. The cryptography of public-key or asymmetric cryptography. The generation of such keys depends on cryptographic algorithms based on mathematical problems to get one-way functions. Only a private key requires sufficient protection to be kept private; the public key can be released anonymously without giving specifics. In such a scheme, some human beings may encrypt a message using the receiver's public key, but the encrypted message can only be decrypted with the receiver's private key. This facilitates a server to create a cryptographic key for symmetric-key cryptography and to use a client's openly shared public key to encrypt the new entity's symmetric key.

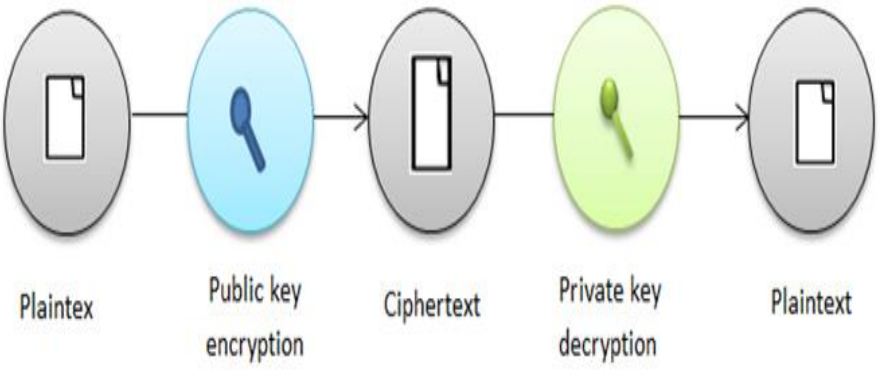

Figure 3. Asymmetric Key Cryptography

Therefore the server can connect this encrypted symmetric key to the client on unsecured channels, and only the client can decrypt it using the client's private key pair to the public key used by the server to encrypt this code. With both the client and the server now using the same symmetric key, they can potentially escalate to symmetric key encryption to otherwise securely communicate back and forth unprotected

networks. It has the option of not having to manually pre-shared symmetric keys, while also having the advantage of symmetric-key cryptography for better information throughput over asymmetric key cryptography. Robust authentication with public-key cryptography is also practicable. To create a short digital signature on the message, a message is linked with a private key by the sender. Anyone with the corresponding public key of the sender may couple the same message and the alleged digital signature associated with it to establish if the signature was genuine, i.e. given by the owner of the corresponding private key.

Public key algorithms are important safety ingredients in modern cryptosystems, applications, and protocols that safeguard the confidentiality, authenticity, and non-reliability of electronic communications and data storage. Various dating strategies rely on themselves, such as Transport Layer Defense (TLS), S/MIME, PGP, and GPG. Some public-key algorithms provide key distribution and transparency (e.g., Diffie-Hellman key exchange), some provide digital signatures (e.g., Digital Signature Algorithm), and some provide both (e.g., RSA). In preference to besides it, asymmetric encryption is weak for some purposes. The cryptosystems of today use both symmetric and asymmetric encryption (such as TLS, Stable Shell).

4. SECRET SHARING PROTOCOLS

Splitting and revealing key algorithm statistics is a specific branch of cryptography. Inside the most general case, their objective is to generate this same kind of part of the knowledge in question that should be reported by many other sanctioned figures. What exists here is the problem of distinguishing events in a form that facilitates. Its reconstruction by a particular candidate of n-persons interested in reassembling the split data. What develops here is the problem of dividing data in a way that helps its reconstruction by a given group of n-persons oriented in the processing of information that is split. Established solutions for algorithms to accomplish this at the same time, the aim should determine that none of the groups of participants in such a protocol, whose number is lower than the number of m persons required, could read split message interpretation.

The information spanning algorithms allow it to be split into chunks known as shadows that are later distributed among the protocol participants such that certain shares are owned by certain user sub-sets are capable, when combined of reconstructing the new data. There are two major classes of relevant data algorithms, in other things, confidential separation and secret contact. In the first technique, data is conveyed among the protocol participants, and all the participants, participants are anticipated to deliver their elements together to get it fixed. A more universal procedure of the latter strategy is to divide information i.e. sensitive information. In this scenario, the information is received here too, among the participants of the protocol, yet to have it enough, reconstructed, to have a certain number of specified constituent shares when constructed the scheme. The other type of splitting method is the techniques for sharing information. They are information methods of distribution, which are often more technical. It is also acknowledged that algorithms for knowledge transfer areas schemes of threshold

Using such a platform enhances taking and splitting any detail into n Parts known as shadows are voluntary. In such a way, that any m (where m/n) may be from among them. The dataset is used to rebuild it. This is the (m, n)-threshold scheme named below, these findings show an algorithm for expanding the scope with certain networks and systems generation in the form of a single additional shadow communication details required for the reconstruction of an entirely elusive secret. The overall procedure of using the grammatical basis for the development of the threshold systems are as follows:

- The opportunity of one of the classical systems for the top-secret exchange
- The transition of the source data to the form string of bits
- Grammar specification that activates each bit place for exclusive input (data)
- To decipher the bit using a syntax monitoring system, a sequence
- Acquisition of a production numbers sequence

grammatical rules), which may be the endpoint of parsing

- Segregating the question represented by a succession of

numbers of growth, with the application of the threshold scheme chose

- Shadow distribution here between participants the Protocol

5. DISK ENCRYPTION

Disk encryption refers to the technology of encryption that encrypts data on the drive of a computer's hard drive. In either software (see encrypting software or hardware, file system generally consists of (see disk encryption hardware). Disk encryption is also referred to as OTFE or clear encryption (On-the-fly Encryption).

6. APPLICATION AND HARDWARE-BASED PRIVACY SECURITY

To protect it from theft, software-based security solutions encrypt the data. However, in terms of providing it unrecoverable, malware or a hacker would corrupt the data, rendering the device unusable. Hardware-based security devices eliminate data access from speaking and listening, thereby presenting very effective support from tampering and unauthorized disclosure. Security based on hardware or encouraged computer security is an alternative to computer security only for technology. Due to the physical access needed to be compromised, encryption tokens such as those using PKCS#11 might even be healthier. Working off hardware-based security: Through manual activities, a piece of equipment allows a user to log in, log out and set varying degrees. To ensure proper users from logging in, logging out, and varying privilege levels, the program uses biometric technology. As operating systems are exposed to malicious attacks by viruses and hackers, hardware-based access control is more important than the risk posed by operating systems.

After malicious updates are made, the data on hard disk drives may be abused. The software will not influence the user privilege levels with hardware-based authentication. A hacker or a malicious code is unable to gain access to secure console data or execute unauthorized privileged operations. Only if the hardware itself is malicious or has a vulnerability is this concept broken. The hardware preserves the layout of the operating system and the powers of the file system from manipulation. Using a combination of hardware-based defense and safe system administration policies, a completely accessible system can therefore be generated.

7. DATA BACK UP

To ensure how data that is lost can be rescued from another source, backups are used. In most industries, it is considered significant to keep a backup of any data and the approach is recommended for any files of concern to a user.

8. DATA MASKING

Structured data masking is the mechanism of obscuring (masking) particular data inside the same database table or cell to ensure that data privacy is upheld and that unnecessary personnel is not exposed to sensitive information. It could include masking user data, for example, as then members of banking customers can only see the last 4 digits of a national identifier for customers), developers (who need actual production data and evaluate mobile app releases but should not be able to see sensitive financial data), outsourcing companies, etc.

9. DATA ERASURE

Data erasure is a software-based overwriting technique that entirely wipes all digital information residing on a hard drive or other digital media to ensure that when an asset is replaced or reused, no valuable data is lost.

10. IDENTITY-BASED SECURITY

A critical primitive dimension of ID-based cryptography is D-based encryption or identity-based encryption (IBE). As such, it is a form of public-key encryption in which some specific person notices a significant is the public key of a user (e.g. the email address of a user). This means that a sender who has access to the commonly applied voltage would use the text value of the target name or the email address as a key to encrypt a message, for example. A central authority possesses the decryption key from the decryption key user, as it extracts essential keys for every user, it needs to be trusted. Identity-based systems allow any human to generate a public key from a known identity value, like just an ASCII string. The corresponding private keys are developed by a trusted third party, called the private key Generator (PKG). The PKG first publishes a public key master and continues the corresponding private key master to survive (referred to as master key).

Given the master public key, by merging the master public key with the importance of identity, any party can compute a public key corresponding to the identity. The party enabled the PKG to use the identity ID contacts to obtain the corresponding private key, which uses the master private key to retrieve the private key for the identity ID. As an effect, with no prior distribution of keys between individual participants, parties can encrypt messages (or verify signatures). This is helpful in the diagnosis were caused by technological regulations, pre-distribution is inconvenient or infeasible for authenticated keys. However, the appointed person must receive a private key from the PKG in particular to decrypt or sign messages. A caveat to this policy is that, as it is the PKG must be highly trusted. can acquire the private key of any user and can therefore decrypt (or sign) messages without approval. Since the private key of any user can be obtained by using the secret of the third party, this system has inherent key escrow. A variety of variant frameworks,

including certificate-based encryption, ensuring a safe issuing cryptography, and certificate-less cryptography, have been intended to eliminate the escrow.

Linguistic leadership development procedures guard the secret by separating it within a party of its trustees and by describing it etymologically. The contents of a secret like this. Through the deployment of linguistic data interpreting methods, contained in the described grammatical formalisms, the content of the data it's necessary to analyze the secret protocols for message-sharing. This protocol class stimulates secret information not only to be preserved but also analyzed semantically. This is crucial because of the validity of this evidence. The more understanding the more permissible type of information sharing is the arbiter responsible for the information sharing process if they should introduce the protocol. The appropriate level of shadows must be combined to simulate the message content in the case of linguistic data-sharing protocols. The number of shadows acceptable to regenerate at the stage of its design and that actual secret is specified in the message-sharing protocol. In the phrase the following message-sharing protocols to reconstruct the secret information.

- Combining the number of shadows available, except the shadow supplying the linguistic information: the secret knowledge will be the secret content. A generic (m, n) threshold operation, restructured without knowing the linguistic evidence
- Combining the number of shadows expected, including the shadow containing linguistic information: The secret content, including the content of the secret, a linguistic professional development structure will be reconstructed and linguistic information will be reconstructed.
- Combining the number of shadows produced, which includes only a subset of the shadows developed as a medium of learning Information Protocol Splitting: The mystery substance will be reconstructed, while the linguistic information reconstruction will depend on the number of combined shadows of the linguistic communication channel. if this number is necessary for the lexical items, knowledge to be rebuilt, then the database will be reconstructed. Otherwise, it is not meant to be restored.

For communication protocol, linguistic protocols are used to

- Working to ensure the reliability of the secrets disclosed
- ensure also that linguistic data collected in this type of protocol is guarded, and
- Taking good care of the meaning of the secret (this meaning can be assessed using an interpretation of data classification and linguistic techniques)

Linguistic protocols for sharing information not only safeguard the secret from disclosure but also allow the shared information to be shared to be viewed. A secret and needs to be understood. Data splitting processes enhanced with semantic elements understanding of protected intelligence enable this kind of solution is an effective way for storing information from various significance and works.

11. RESULTS

The "Text" classified sensitive text message is encrypted into 15 separate videos and then secret, to be understood and assessed, as suggested based, via reference. To explain this elaboration, chose 10 PC cover-videos of multiple lengths and found the findings. The results of this experiment are specified in table 1. For 10 PC videos with just a varied variety. The integrity of the responsive, concealed in pictures, unknown testing research cover leading to changes in bits based on the LSB option used as mentioned in table 1. Some findings the percentage estimate of vulnerability was made up of per video and efficiency using the protection of each video as analyzed by PSNR (Peak Signal to Noise Ratio) on a formula core principle:

$$PSNR = 20 \log_{10} MAI / \sqrt[4]{SD} \quad (1)$$

Where the cumulative strength MAI refers to the resolution given to every pixel, i.e. this MAI, this MAI in the images, the value is 255. Likewise, on the other hand, the square of the difference is classified as MSE. (the distortion) between the original cover and the original cover for Stego. From the inside of the cover, the contrast can be the formula below are always assessed using this MSE

$$MSE = \sum_{j=1}^{all\ pixels} \sum_{all\ pixels}^{i=0} \text{stegnography}(j - i)2 \text{ - cryptography (i-j)} \quad (2)$$

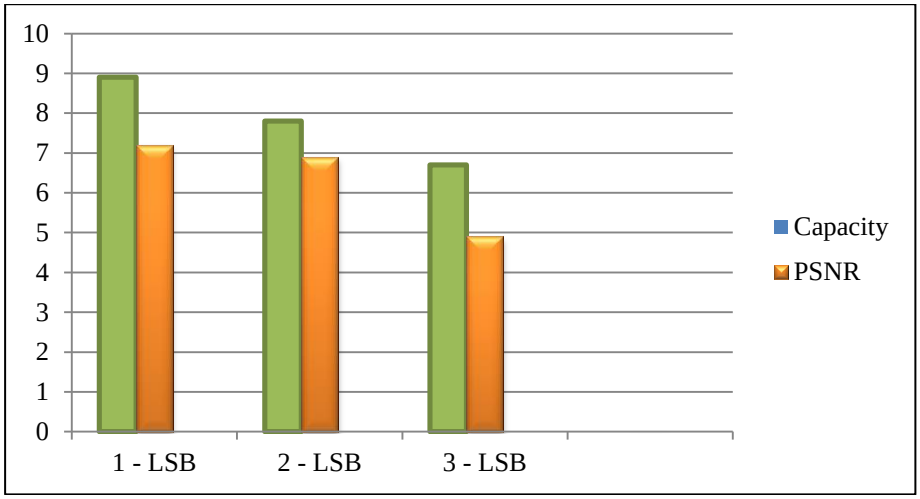

Figure 4. Comparison between 1,2,3 - LSB

Above figure 4. Shows the comparison between 1,2,3 LSB. The per-video efficiency, i.e. stego cover-media, the sum of detail that can be measured is estimated as without

being substantially concealed in the video log, adjust that. According to the cover, it is assessed used, that is.

Table 1. Encrypt TEXT in 10 different videos

Frame Size	Video Size(kb)	1 - LSB		2 - LSB		3 - LSB	
		Capacity	PSNR	Capacity	PSNR	Capacity	PSNR
142*188	329	73,057	55.63	185.09	59.78	228.05	69.07
135*158	477	66,082	47.33	489.40	42.09	347.04	22.18
176*188	368	58,076	59.90	558.69	52.28	689.01	78.04
189*140	782	38,249	25.39	487.06	66.07	776.05	88.48
197*158	825	47,015	65.36	558.48	80.06	448.07	58.03
228*117	982	66,08	47.09	669.28	93.08	889.06	55.29
328*144	447	70,09	59.14	712.05	79.07	929.26	38.04
479*158	698	88,89	63.59	479.98	45.85	897.06	77.09
669*144	557	78,49	79.36	892.07	96.28	859.17	89.69
789*188	489	49,82	97.39	881.59	79.99	871.09	95.08

The role of using the 2-layer was studied in this work important text protecting scheme in PCs assuming capacity and security. All tests were assumed to be hiding, i.e. stego-embedding the sensitive data of fixed, encrypted text " sensitive data in 10 different videos using "Text Various LSBs. 1LSB, 2-LSB, 3-LSB are the LSBs already described to disguise the secret data in youtube clips with positive approaches can as seen in Table1, the video. The LSB used is directly proportional to defense and inversely proportional to health, competitive with as to. Like the number of bits to mask the change in data (1LSB, 2-LSB, 3-LSB), as clearly fit perfectly 1-LSB, taking decisions and vastly increased protection: low capacity and high security: 2-LSB: medium capability and medium stability, 3-LSB: low hazard and long lifetime, as indicated. It's from there to be acknowledged, the real indication of stability and power is that fully depending on the LSB and videos used, can be retrieved and can not be predicted within the PC or even estimate.

12. CONCLUSIONS

In necessary to defend the place to protect the ideas of information concealment is used for maximum access to information, in part by unauthorized persons. This technique is utilized using consistent cryptographic algorithms to enhance overall security and privacy. Exposes this paper as a method of distinguishing secret data within a local company of broken secret trustees. This approach is aimed at distinguishing. Both elements of the proprietary material just inside the holders' band. The information splitting protocol is used to escape a condition where only one trustee retains private data. Inside of the confidential trustee network, the method of distributing a secret message defends data from a single individual's report. Only by combining the equivalent number of shadows can the universal conscience of things be reconstructed. In this segment, linguistic algorithms for data sharing are also discussed. The essence of this solution is to generate an imaginary shadow that understanding that is linguistic. This shadow is

divided between shadow holders, along the remaining parts of the group secret are shared with. possible applications of the services mentioned are seen in semantic knowledge management systems in which it is possible to decide semantic layers and any secured system (secret). Numerous methods of crypto will be cross-checked as asymmetrical as well as symmetrical. Planning is also to be carried out to analyze various other ways to boost the capability and protection of kit for internal use of applications for PCs. To support other languages and their capabilities, the application can be further upgraded, which may some more focused analysis is needed.

REFERENCES

[1] N. Al-Otaibi, & A. Gutub, "2-Layer Security System for Hiding Sensitive Text Data on Personal Computers", Lecture Notes on Information Theory, Engineering and Technology Publishing, Vol. 2, No. 2, pp. 151-157, June 2014

[2] N. Al-Otaibi, & A. Gutub, "Flexible Stego- System for Hiding Text in Images of Personal Computers Based on User Security Priority", Proceedings of 2014 International Conference on Advanced Engineering Technologies (AET-2014), December 2014, pp. 250-256.

[3] A.Gutub, "Pixel Indicator Technique for RGB Image Steganography", Journal of Emerging Technologies in Web Intelligence (JETWI), Vol. 2, No. 1, pp. 56-64, February 2010.

[4] N. Al-Otaibi, A. Gutub, & E. Khan, "Stego- System for Hiding Text in Images of Personal Computers", The 12th Learning and Technology Conference: Wearable Tech/Wearable Learning, Effat University, April 2015.

[5] https://www.merriam-webster.com/dictionary/steganography

[6] Fridrich, Jessica; M. Goljan; D. Soukal (2004). Delp Iii, Edward J; Wong, Ping W (eds.). "Searching for the Stego Key" (PDF). Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VI. Security, Steganography, and Watermarking of Multimedia Contents VI. 5306: 70–82. Bibcode:2004SPIE.5306...70F. doi:10.1117/12.521353. S2CID 6773772. Retrieved 23 January 2014.

[7] Pahati, OJ (2001-11-29). "Confounding Carnivore: How to Protect Your Online Privacy". AlterNet. Archived from the original on 2007-07-16. Retrieved 2008-09-02.

[8] https://sci-hub.se/10.1515/nleng-2015-0013

[9] Ogiela, U., & Ogiela, L. (2018). Linguistic techniques for cryptographic data sharing algorithms. Concurrency and Computation: Practice and Experience, 30(3), e4275.

[10] Hamzah, A. A., Khattab, S., & Bayomi, H. (2019). A linguistic steganography framework using Arabic calligraphy. Journal of King Saud University-Computer and Information Sciences.

[11] Xiang, L., Wu, W., Li, X., & Yang, C. (2018). Linguistic steganography based on word indexing compression and candidate selection. Multimedia Tools and Applications, 77(21), 28969-28989.

[12] Xiang, L., Yu, J., Yang, C., Zeng, D., & Shen, X. (2018). A word-embedding-based steganalysis method for linguistic steganography via synonym substitution. IEEE Access, 6, 64131-64141.

[13] Taha, M. S., Rahim, M. S. M., Lafta, S. A., Hashim, M. M., & Alzuabidi, H. M. (2019, May). Combination of steganography and cryptography: A short survey. In IOP conference series: materials science and engineering (Vol. 518, No. 5, p. 052003). IOP Publishing.

[14] Zhou, T., Shen, J., Li, X., Wang, C., & Shen, J. (2018). Quantum cryptography for the future internet and the security analysis. Security and Communication Networks, 2018.

[15] More, S. S., Mudrale, A., & Raut, S. (2018, January). Secure Transaction System using Collective Approach of Steganography and Visual Cryptography. In 2018 International Conference on Smart City and Emerging Technology (ICSCET) (pp. 1-6). IEEE.

[16] Chakraborty, S., & Kar, N. (2018). An Approach Towards Linguistic Steganography. International Journal of Computational Intelligence & IoT, 2(4).

[17] Bache, F., Plump, C., Wloka, J., Güneysu, T., & Drechsler, R. (2019). Evaluation of (power) side-channels in cryptographic implementations. it-Information Technology, 61(1), 15-28.