SmallSEOTools

PLAGIARISM SCAN REPORT

Words	1000	Date	August 12,2020
Characters	6218	Exclude Url	

0%	100%	0	55
Plagiarism	Unique	Plagiarized Sentences	Unique Sentences

Content Checked For Plagiarism

But the key is the weakest point in order to secure that SHA-256 (Secure Hash Algorithm) will be used that will give a hash value. Hash is “not encryption” because it can never be decrypted back to the initial text, it a one-way street. This makes the system robust and patches the weakest link. The Secure Hash Algorithm (SHA-256) is a part of the family. The cryptographic hash functions was produced by the “National Institute of Standards and Technology” as a U.S. Federal Information Processing Standard. SHA-256 is patented in US patents 6829355. Hash is not “encryption” because it can never be decrypted back to the initial text. It is of fixed length for any varying length of the source text. SHA-256 is achieved by the following steps like padding, append length, divide the input into 512-bit blocks, add chaining variable, process block respectively. SHA-256 generates a unique 256-bit or we can say 32-byte of hash code. It does 64 rounds in order to reach to the final hash value. Any text length will also be transformed into a digest size of 256 bits (32 bytes). 16.80 cycles per byte on 64-bit processor x86 architecture. It has 64 iterations in one cycle. Which makes it more safe and secure. 1.1 Purpose The goal of steganography is covert communication. So, an elementary requirement of this steganography system is that the covert message carried by stego-media should not be sensible to human beings. The secondary target of steganography is to avoid drawing suspicion to the existence of a hidden message. This approach of information hiding technique has recently become important in several application areas This project has the following objectives: • To provide security tool based on image steganography techniques. • To explore techniques of hiding data using hide module of this project • To extract techniques of getting secret data using the retrieve module. Steganography comes into play where encryption is not permitted. Or, more precisely, steganography is used to addendum encryption. An encrypted file can be concealed using steganography, so even if the encrypted file is deciphered, the hidden message is not seen or vice versa is also possible. Steganography hides the data inside the image no one able to notice that this image will be containing some crucial information but even if someone detects that the image contains the data inside it, the data will be protected with the encryption. The image will only be having the cipher text embedded with it. For decrypting that cipher text the user will be needing the key without it, it is impossible to get the information. Scope The system hides the classified information into an image in order to secure the data and make communication of data undetectable and enhancing its security by using Advance Encryption Standard (AES-256) and even securing the weak link that is the key with SHA-256. It will make the system impenetrable would having rightful access. This system could help the Government agencies and National Security agencies in order to secure the classified information. 1.3.1 Definition, Acronym and Abbreviation The project is the digital information security system used for securing the classified text. The modules such a hide, retrieve and key creation module depicts the functionality of the application. The Earlier form of linguistic or language of hidden writing. Then later in series, such as invisible ink are used to hide messages physically. One drawback of linguistic steganography is that users must have skilled themselves to have a good knowledge of linguistry. In recent years, everything is trending toward digitization. And with the development of internet technology, digital media can be transmitted conveniently over the network. Therefore, messages can be secretly carried by digital media by using steganography techniques and then be transmitted through the internet rapidly. Steganography is a technique of hiding the fact that communication is taking place, by hiding information in other information. Many different cover file formats can be used, but digital images are trending because of their frequency on the internet. For concealing classified data into images,

there are various steganography techniques some are more complex than others and all of them have respective strong and weak points. So, we create this application, to make the data hiding simpler and user friendly. Least Significant Bit (LSB) is a steganography technique embeds the data into the cover image or target image. This technique is implemented by making changes in the least significant bit (LSB) of a byte. LSB provides the least change in the image which is far from persistent of a human naked eye. The change in a byte is 0.000002% which is almost negligible. Secure Hash Algorithm (SHA-256) is a part of

human naked eye. The change in a byte is 0.000002% which is almost negligible. Secure Hash Algorithm (SHA-256) is a part of the family. The family of cryptographic hash functions which was declared by the National Institute of Standards and Technology as a U.S. Federal Information Processing Standard. SHA-256 is patented in US patents 6829355. Hash is “not encryption” because it can never be decrypted back to the initial text. It is of fixed length for any varying length of the source text. SHA-256 is achieved by the following steps like padding, append length, divide the input into 512bit blocks, add chaining variable, process block respectively. SHA-256 generates a unique 256-bit or we can say 32-byte of hash code. It does 64 rounds in order to reach to the final hash value. Advance Encryption Standard (AES-256) is a symmetric key encryption technique, which uses only one secret key to cipher(encrypt) and decipher(decrypt) data. AES-256 uses a key length of 256 bits, it uses the largest bit length and is practically adamantine by brute force attack on the basis of current computing power, which makes it the strongest encryption standard. The AES encryption method first performs substitution of data using a substitution table; which is followed by shifting of data rows, then after that mixing of the columns takes place, and finally the last transformation with a simple exclusive (XOR) operation performed on each column using a different part of the encryption key.

Sources	Similarity