VIT®

Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

CSE3502 – Information Security Management

Project Title

Data Security Using Cryptographic-Steganography

Submitted under:

Prof. Murali S

Associate Professor Grade 1 School of Computer Science and Engineering

Submitted by:

Name	**Registration Number**
Malvika Singh	**20BCE0857**
Boggavarapu Ch N V Shivani	**20BCE0563**
Kartikey Saini	**20BDS0040**

Index

Abstract

The use of digital communication tools for data and information exchange is growing along with the development of the internet. However, despite the fact that such a network is the most well-liked for its quick and simple method of exchanging information over great distances, message transmissions over the Internet continue to have a variety of security issues. Because of this, the applications of the cyber world require a high level of protection for sensitive data, which has caused the field of information hiding to grow rapidly. Two of the most frequently employed methods for protecting digital data are cryptography and steganography. The use of codes to secure information and communications in such a way that only the intended recipients can decipher and process them is known as cryptography. Steganography is a technique for obfuscating secret information by enclosing it in a regular, non-secret file or message; the information is then extracted at the intended location. Steganography can be used in addition to encryption to further conceal or protect data. In this we will basically use an amalgamation of cryptography and steganography and compare the results according to the different algorithms to increase the security of the data.

Introduction

According to recent research findings and analyses that have been published, symmetric and asymmetric encryption algorithms are used to protect data. They accomplish this by transforming the data into new formats that are nearly impossible for unauthorized parties to decrypt or break. The oldest and simplest types of encryption are symmetric ones, like 3DES or AES, which encrypt and decrypt data using just one special secret key. The fact that the sender and receiver share the key is a significant disadvantage because it allows an attacker to listen in on the key exchange channel and use it to decrypt the data. The secret key must be transmitted over a secure channel between the sender and the receiver. On the other hand, asymmetric encryption, like RSA, encrypts data using two keys: a public key and a private key. Although the private key is kept private and is used to decrypt the message, anyone with the public key can use it to send a message. This method improves security. Overall, they all entail converting plain text into ciphertext and vice versa. The various algorithms used in cryptography are shown in the diagram below.

Triple Data Encryption Standard (3DES)

Data Encryption Standard for Ripple (3DES) ANSI X9.17 and ISO 8732 [11] both standardise the Triple Data Encryption Standard (3DES), also known as the Triple Data Encryption Algorithm (TDEA), which was first proposed by IBM in 1998. The purpose of this encryption algorithm is to fix the flaws in its predecessor, the DES, without necessarily developing a brand-new algorithm. The three-key triple DES (K1, K2, and K3) and the two-key triple DES (K1 and K3) are the two variations, and they both employ 56-bit keys. As can be seen in the figure below, it is a symmetrical block cypher that applies the DEScipher algorithm three times to each block of data. When compared to other cypher methods, it is reportedly slower.

Advanced Encryption Standard (AES)

It's time to replace the outdated DES and 3DES encryption algorithms with the new AES, as stated in the 1997 NIST announcement calling for cypher candidates to implement a new encryption standard [11]. AES is a preferred option for many because of its faster encryption speed and improved security. In actuality, its length-variable keys take the place of the tiny 3DESkeys. It is also a huge amount faster. AES can be categorised as AES-1 (128-bit key-length), AES-192(192-bit key-length), or AES-256 depending on the key length (256-bits key-length). The AES system uses ten rounds for 128-bit keys, twelve rounds for 192-bit keys, and fourteen rounds for 256-bit keys, as shown below. Multiple transformations are applied to plain text, including byte substitution, shiftrows, mix columns, and add round key transformations. Its key length flexibility is advantageous during software implementation in Java and C programming, as well as in hardware and software . However, because of the larger block size and the straightforward mathematical structure, it requires more resources and processing power, which is its main drawback.

Rivest-Shamir-Adleman(RSA)

Adleman and Rivest-Shamir (RSA) In 1978, Ron Rivest, Adi Shamir, and Leonard Adleman developed RSA. It is a well-known public key encoding system for key exchange, digital signatures, and database encryption. operate using an encryption block and a variable key. When using block size data, it integrates plain text and cypher text between 0 and 1. Compared to other algorithms, RSA has improved security, which is its main benefit. It is actually one of the safest algorithms. The slow encryption speed, difficult to create keys, and vulnerability to attacks are its main drawbacks. There are three steps: creating a public/private key pair, converting the data's plain text into ciphertext, and decrypting the data.

Objective

Security is the most important task in any communication. The advancement of technology and the widespread use of the World Wide Web for communication raises security concerns. However, the challenges are manageable with advanced secure network technologies, but these technologies are not always reliable for communicating secrete information over long distances, necessitating the use of additional security mechanisms to secure secret information. There are a lot of algorithms created for cryptography, the most commonly used ones are Triple Data encryption Standard (3DES), RSA, AES Steganographic techniques like Least Significant Bit (LSB) is a mathematical function used to change the image spatial domain to the frequency domain. Both steganography and cryptography offer security, but no single technique can effectively secure information, and various security categories have various needs and issues.

Literature Survey

Paper Title	**A Review Paper on Cryptography**
Citation	A. M. Qadir and N. Varol, "A Review Paper on Cryptography," 2019 7th International Symposium on Digital Forensics and Security (ISDFS), Barcelos, Portugal, 2019, pp. 1-6, doi: 10.1109/ISDFS.2019.8757514.
Work Done	Cryptography is a technique for ensuring message confidentiality. Various algorithms and methods have been developed to achieve this level of security. This paper sheds light on historical and contemporary algorithms.
Techniques Used	Historical Algorithms × Caesar cipher × Simple Substitution cipher × Transposition Modern Algorithm × Stream ciphers × Block ciphers × Hash function × Public key system

Observatio n	Cryptography is essential in achieving the primary goals of security, such as authentication, integrity, confidentiality, and no-repudiation. In this paper, we demonstrated a review of some of the research that has been conducted in the field of cryptography, as well as how the various cryptographic algorithms used for various security purposes work. Cryptography will continue to emerge in IT and business plans to protect personal, financial, medical, and ecommerce data while also providing a reasonable level of privacy.

Paper Title	**A Survey on Symmetric and Asymmetric Cryptography Algorithms in information Security**
Citation	A Survey on Symmetric and Asymmetric Cryptography Algorithms in information Security M. A. Al-Shabi* *Department of Management Information System, College of Business Administration, Taibah University, Saudi Arabia, mshaby@taibahu.edu.sa DOI: 10.29322/IJSRP.X.X.2018.pXXXX
Work Done	This paper discusses a number of significant algorithms that are used for the encryption and decryption of data across all fields in order to conduct a comparative analysis in terms of speed (implementation) and security (special keys).

Techniques Used	**Symmetric Cryptography** × Data Encryption Standard (DES) × Triple Data Encryption Standard (3DES) × Advanced Encryption Standard (AES) × Blowfish × Hybrid Cubes Encryption Algorithm(HiSea) × Rives Cipher 4 (RC4) × Tiny Encryption Algorithm (TEA) × CAST × Twofish × Serpent × RC2 **Symmetric Cryptography** × Rivest-Shamir and Adleman (RSA) × Diffie-Hellman × Elliptic Curve Cryptography(ECC)

Observation	AES clearly outperforms RC2, DES, and 3DES in the symmetric category, especially in terms of time consumption. 3DES performs poorly on this metric, owing to its triple phase encryption approach. Furthermore, discussions in this category reveal that the key size affects both battery and time consumption. In terms of encryption speed and attack susceptibility, the Diffie-Hellman algorithm outperforms RSA in the asymmetric category. Overall, the choice of a cypher method should be determined by specific needs rather than general perception, because algorithm vulnerabilities are not weaknesses in all implementation scenarios.

Paper Title	**Lightweight cryptography in IoT networks: A survey**
Citation	Muhammad Rana, Quazi Mamun, Rafiqul Islam, Lightweight cryptography in IoT networks: A survey, Future Generation Computer Systems, Volume 129, 2022, Pages 77-89, ISSN 0167-739X, https://doi.org/10.1016/j.future.2021.11.011

Work Done	Cryptography is used to secure network authentication, confidentiality, data integrity, and access control. Traditional cryptographic protocols, however, are no longer suitable for all IoT environments, such as smart cities, due to the many constraints of IoT devices. This paper discusses cutting-edge lightweight cryptographic protocols for IoT networks and provides a comparison of popular modern cyphers.
Techniques Used	Lightweight algorithms used to secure IoT network communications in detail. Lightweight × Block Ciphers (LWBC) × Lightweight Stream Ciphers (LWSC) are two types of symmetric lightweight algorithms (LWSC).
Observation	Each algorithm has merits and demerits in terms of ensuring security while exchanging information in the IoT environment. Some algorithms demand more storage space but have fewer computational requirements and vice versa.

Paper Title	**Dual Layer Security of data using LSB Image Steganography Method and AES Encryption Algorithm**
Citation	S. Singh and V. K. Atria, “Dual layer security of data using LSB image steganography method and AES encryption algorithm, ” International Journal of Signal Processing, Image Processing and

	Pattern Recognition, vol. 8, no. 5, pp. 259–266, 2015. DOI: http://dx.doi.org/10.14257/ijsip.2015.8.5.27
Work Done	The digital photograph Steganography is the science of concealing sensitive information in another medium of transmission in order to achieve secure and confidential communication. In this paper, we present a dual layer of data security, in which the first layer encodes data using Least Significant Bit image steganography and the second layer encrypts data using the Advance Encryption Standard Algorithm.
Techniques Used	The work presented how to provide sensitive data with dual layer security. To achieve the desired results, we combine steganography and cryptography (encryption/decryption). The system is built on the Java platform with the Netbeans IDE. For image steganography, we used the simplest yet most effective method known as the LSB image steganography algorithm. We used the error-free AES encryption algorithm for the encryption/decryption layer. In the future, we hope to improve the steganography layer by enhancing the current LSB algorithm.
Observatio n	All three possible images are observed, namely the cover image, the stego image, and the encrypted stego image. There is no distinction between the stego and cover images. Nobody can see the use of steganography to hide data in cover images, and the changes are so minor that the human eye can't even see them. Changes to the image are made at the pixel level, which results in high security.

Paper Title	**DUAL LAYER DATA HIDING USING CRYPTOGRAPHY AND STEGANOGRAPHY**
Citation	Dipesh G. Kamdar1, Dolly Patira2, Dr. C. H. Vithalani3 1Department of Electronics and Communication, JJ Tibrewala University, Jhunjhunu, Rajasthan, India – 333001. Department of Computer Engineering, VVP Engineering College, Rajkot, Gujarat, India - 360005 3Department of Electronics and Communication, Government Engineering College, Rajkot,Gujarat, India – 360005 International Journal of Scientific Engineering and Technology www.ijset.com, Volume No.1, Issue No.4, pg :134-138 https://ijset.com/publication/v1/115.pdf
Work Done	Steganography and cryptography are two popular methods of secretly exchanging information. Steganography conceals the message's existence, while cryptography distorts the message itself. Whether cryptography or steganography is used, there is always the possibility that the hidden message will be discovered. This paper proposes a dual layer hiding technique for faithful and secure communication.
Techniques Used	To conceal information, the proposed algorithm combines cryptography and steganography. Cryptography is used to turn information into garbage, which is then hidden in cover video using steganography. As a result, no Brute Force methods or steganalysis tools can uncover the hidden information.

Observation	Figure depicts the outcome of image cryptography using a public key. Figure depicts the resulting image of Steganography using the discrete cosine transform (DCT). It is clear that cryptography produces a garbage image, whereas Steganography produces an image that appears to be the original image. The combination of cryptography and steganography, known as crypto-steganography, along with the presence of a public key and a private key, results in the safest method for passing secure information over any communication channel.

Paper Title	**Performance Analysis of Cryptographic Algorithms in the Information Security**
Citation	M. Panda, "Performance analysis of encryption algorithms for security," 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), Paralakhemundi, India, 2016, pp. 278-284, doi: 10.1109/SCOPES.2016.7955835.
Work Done	The encryption of data through the use of various data encryption algorithms will add security to the data being transmitted. This paper primarily compares (AES, DES, 3DES, BLOWFISH, RC4), Asymmetric (RSA, DSA, Diffie-Hellman, EI-Gamal, Pailier), and Hashing (MD5, MD6, SHA, SHA256) algorithms.

Techniques Used	Symmetric Algorithms × DES × 3DES × BLOWFISH × RC5 × AES Asymetric Key Cryptographic Algorithms × RSA × DSA × Diffie-Hellman × Elgammal Discuss the advantages and disadvantages of asymmetric and symmetric key algorithms. According to the survey, the security of RC5 and RC4 is questionable, but RC4 is faster than RC5. These AES encryption algorithms are more secure, efficient, and faster than all other algorithms because they support 256-bit key sizes and protect against future attacks. Twofish took the place of Blowfish.
Observation	Although RSA is the best asymmetric key algorithm, it takes longer to encrypt data and has difficulty decrypting large integers. The outcome demonstrates that Blowfish and AES outperform the competition. When compared to the other algorithms mentioned above, AES is the most effective and secure algorithm

	with a small key size. The highly secure encryption algorithm AES is finally accepted with a larger key size.

Paper Title	**A Comparative Study of Symmetric Cryptography Mechanism on DES, AES and EB64 for Information Security**
Citation	K. Logunleko, O. Adeniji, and A. Logunleko, “A comparative study ofsymmetric cryptography mechanism on des aes and eb64 for informationsecurity,” Int. J. Sci. Res. in Computer Science and Engineering, vol. 8,no. 1, 2020.
Work Done	The shared and sensitive data has been secured and protected using a variety of techniques. This study mainly focused on using cryptography to guarantee that there is no room for data transmission security breaches. However, the Private or Secret Key Encryption Infrastructure needs to be adopted as the model to implement security in order to increase the security and effectiveness of valuable data. Based on an analysis of the encryption and decryption time allotted at each different experimental stage, this research work implemented three encryption techniques, including DES, AES, and EB64 algorithms, and compared their performances on both encryption and decryption techniques.
Techniques Used	Nine (9) factors—Key Size, Block Size, Scalability, Algorithm, Encryption, Decryption, Power Consumption, Security, Key Used, Rounds, Hardware and Software Implementation—were taken into account in a comparison study between DES, AES, and EB64. A minimum of a 2.0 GHz processor, 2 GB of RAM, and 16

	GB of storage space were used to implement the developed comparison model using sublime text, Javascript, HTML5, mobile phones, and Phonegap technology. The three aforementioned algorithms' performance was assessed using the parameters of encryption and decryption time.
Observation	The effectiveness of each algorithm on a mobile phone was evaluated using the experimental results that were obtained. Results from the various experiments conducted on SMS plaintext indicate that EB64 encryption and decryption took less time than AES and DES. According to the graph's findings, the EB64 algorithm takes the least amount of time to encrypt and decrypt data compared to DES and AES, while DES takes the longest compared to AES and EB64.

Paper Title	**Rotation Left Digits to Enhance the Security Level of Message Blocks Cryptography**
Citation	M. Abu-Faraj, A. Al-Hyari, K. Aldebei, Z. Alqadi, and B. Al-Ahmad,“Rotation left digits to enhance the security level of message blockscryptography,” IEEE Access, pp. 69 388–69 397, 2022.

Work Done	A straightforward approach to message cryptography will be suggested in this research paper. Using this method, a message is divided into blocks of a fixed size. The size of the blocks ranges from 2 to 60. The method creates an array whose size is equal to the number of resulted blocks using a secret colorimage. After that, the array will serve as a private key. In order to apply the block rotation left operation, each element of the private key will be used to determine the associated block's number of rotation digits. The parameters Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Correlation Coefficient (CC), and throughput will be used to evaluate the proposed method. The proposed approach will be contrasted with other widely used message encryption techniques, including Data Encryption Standard (DES), Triple-DES (3DES), Advanced Encryption Standard (AES), and Blow Fish (BF).
Techniques Used	The two fundamental operations that make up the proposed method are implemented. PK generation and mes-sage block rotation are the two operations. An image key that uses a secret colour will be chosen. To create an aPK with a size equal to a message block size, the image must be resized. A number of elements are present in the generated PK. Each element's value will be used as the block rotation value (BRV).
Observatio n	According to experimental findings, the suggested method is sufficiently secure when using a secret image, a large enough block size, and calculated Rotation Left Digits (RLD) for each block. The suggested method will increase the security level of data cryptography based on the following: (1) The image key must be kept secret; (2) The generatedPK size depends on the block size; if the block size is equal to 50 elements, the number of

	combinations needed to hackthe key is equal to (28)50 = 2400; this satisfies the requirement for good key security.

Paper Title	**Hybrid information security system via combination of compression, cryptography, and image steganography**
Citation	Akeel, Wid & Alasady, Ali & Khalaf, Alaa. (2022). Hybrid information security system via combination of compression, cryptography, and image steganography. International Journal of Electrical and Computer Engineering. 12. 6574-6584. 10.11591/ijece.v12i6.pp6574-6584
Work Done	In order to maximise security and capacity, a new system of information hiding within the image was proposed in this paper. The discrete wavelet transform (DWT) algorithm is used in this system to compress the secret image, and the advanced encryption standard (AES) algorithm is used to encrypt the compressed data. To conceal the encrypted data, the least significant bit (LSB) technique has been used.
Techniques Used	When transmitting sensitive data over the Internet, data security and capacity are the most important factors to consider in order to prevent attackers from stealing data and accessing it for a specific purpose. As a result, in this study, we propose a hybrid system for concealing a secret image within another. To improve data security and capacity, this system employs three algorithms: DWT compression, AES cryptography, and LSB steganography. Figures depict the proposed method's hybrid system architecture.

	The proposed method consists of two major phases: embedding and extraction.
Observatio n	The outcomes demonstrate that the suggested system is capable of optimising the structural similarity index and stego-image quality (PSNR value of 47.8 dB) (SSIM value of 0.92). The experiment's findings also showed that using both techniques together maintains stego-image quality by 68%, boosts system performance by 44%, and expands secret data size compared to using each technique separately. The capacity and security of information sent over the internet may be a problem that this study helps to address.

Paper Title	**Combination of Steganography and Cryptography: A short Survey**
Citation	Mustafa Sabah Taha et al 2019 IOP Conf. Ser.: Mater. Sci. Eng. 518 052003 DOI 10.1088/1757-899X/518/5/052003
Work Done	Steganography is the practise of concealing a message (with no traceability) in such a way that it has no meaning to anyone other than the intended recipient, whereas cryptography is the art of converting a plaintext (message) into an unreadable format. Thus, steganography hides the existence of a secret message, whereas cryptography modifies the message format itself. Steganographic and cryptographic techniques are both powerful and resilient. The primary goal of this paper is to examine various methods for combining steganographic and cryptographic techniques to create a hybrid system. Furthermore,

	some distinctions between cryptographic and steganographic techniques were presented.
Techniques Used	Steganography and cryptography have been shown to be insufficient for complete information security; therefore, combining both techniques can result in a more reliable and strong mechanism [45]. Combining these strategies can improve secret information security and meet the security and robustness requirements for transmitting important information over open channels. Figure 5 depicts a strategy for combining both techniques.
Observatio n	After comparing the science of Cryptography and Steganography, the authors cannot guarantee that steganography can be used as an alternative to Cryptography because each aspect has its own peculiarities; Cryptography refers to the act of secret writing through the enciphering and deciphering of encoded messages, whereas Steganography refers to the methods of concealing a secret message into a cover message in such a way that its existence is completely hidden. Using only one of these methods leaves the system vulnerable to a third party. As a result, the combination of Steganography and Cryptography provides increased security and robustness.

Paper Title	**Secure Mobile Computing Authentication Utilizing Hash, Cryptography and Steganography Combination**
Citation	Alotaibi, Muneera & Al-hendi, Daniah & Al Roithy, Budoor & Al Ghamdi, Manal & Gutub, Adnan. (2019). Secure Mobile

	Computing Authentication Utilizing Hash, Cryptography and Steganography Combination. Journal of Information Security and Cybercrimes Research. 2. 10.26735/16587790.2019.001.
Work Done	The work proposes a modification for security authentication systems in mobile devices in this paper.Their enhancement combines hash, cryptography, and steganography mechanisms to secure information transformation over the internet. They used the combination to secure mobile computing and transfer data in a trusted manner. To increase security, the proposed work will use a hash function to store the secret password. The hashed password is encrypted with AES encryption and then hidden within an image to be called back for authentication whenever it is required.
Techniques Used	The goal of this project is to use LSB steganography to encrypt passwords and hide them in a cover image. We used the Android platform and a MySQL database to complete this project. T.Mantoro's [6] technique has a significant flaw in that it stores passwords in clear text in the database, making them vulnerable to database attacks such as SQL injection.
Observatio n	The results demonstrated that combining all security methods provides the best attributes, namely confidentiality, integrity, and authentication. While previous work on the crypto stego method is deteriorating in integrity. A moderate security method can be hash stego functions, which provide all three attributes for quick applications but are slightly less secure than the method involving AES cryptography.

Paper Title	**Enhancing PC Data Security via Combining RSA Cryptography and Video** **Based Steganography**
Citation	Al-Juaid, N.A., Gutub, A.A. and Khan, E.A., 2018. Enhancing PC data security via combining RSA cryptography and video based steganography. Journal of Information Security and Cybercrimes Research, 1(1), pp.5-13.
Work Done	This paper proposed an improved system for securing sensitive text-data on personal computers by combining both cryptography and steganography. The system security is generated by utilising RSA cryptography followed by video-based steganography as two sequential layers to ensure the best possible security while gaining the benefits of both. The study modelled the system and tested it to investigate the relationship between security, capacity, and data dependency. The experiments included testing data security within 15 different size videos, with interesting results. The research emphasised capacity vs. security as an unavoidable tradeoff. The work's uniqueness is demonstrated by displaying various measures that allow the user and application to make the decision.
Techniques Used	To ensure high security appropriate for PC applications, the suggested system employs both cryptography and steganography, taking advantage of the many techniques available. In fact, cryptography and steganography are used as separate layers to provide the best possible security with independent security, capacity, and reliability measures and

	improvements. The cryptography layer employs the RSA crypto algorithm, which is a public cryptographic system based on two keys: one for encryption and one for decryption. The RSA algorithm addresses the issue of key management and distribution.
Observation	The tests detailed the effects of 1-LSB, 2-LSB, and 3-LSB methods on the cover video and provided all possibilities for accepting security. The main result demonstrated the applicability of using a 3-LSB approach to provide acceptable security with practical capacity, making 3-LSB the preferred technique over 1-LSB and 2-LSB techniques.

Paper Title	**Securing Data Transfer in IoT Employing an Integrated Approach of Cryptography & Steganography**
Citation	Ria Das and Punyasha Chatterjee. 2017. Securing Data Transfer in IoT Employing an Integrated Approach of Cryptography & Steganography. In Proceedings of the International Conference on High Performance Compilation, Computing and Communications (HP3C-2017). Association for Computing Machinery, New York, NY, USA, 17–22. https://doi.org/10.1145/3069593.3069605
Work Done	This paper advocates a security scheme that addresses both the aforementioned problems in order to promote secure data transfer in smart IoT environments, using a combined approach of lightweight cryptography and the variable LSB substitution steganography technique. The Variable LSB Substitution scheme

	provides better security than its Simple LSB Substitution counterpart, according to a comparative study that also compares the Simple LSB and Variable LSB Substitution algorithms.
Techniques Used	In the hypothetical situation, the sensor gathers information from the deployed environment and transmits it via LAN to the server for authentication. Then, as depicted in Figure 1, data is transferred to the WAN (for example, to clouds) for storage. The main problem here is any eavesdropping or packet sniffing attack that compromises the confidentiality of transmitted data, especially one that is launched in a LAN network. Algorithms used: Simple LSB Substitution (SLSBS) Embedding Algorithm (SLSBS) Retrieving Algorithm (SLSBS)
Observation	By first encrypting the sensed data using the common encryption algorithm DES, calculating its digest once more using the MD5 algorithm, and then embedding the encrypted data, digest, and key in a different randomly chosen cover image using the Variable LSB Substitution scheme of Steganography technique, we successfully computed all operations (Step 3 of our proposed scheme outlined in Section 3).

Paper Title	**A Novel Technique for Securing Data Communication Systems by Using Cryptography and Steganography**
Citation	Al-Qwider, W.H. and Salameh, J.N.B., 2017. Novel technique for securing data communication systems by using cryptography and steganography. *Jordanian Journal of Computers and Information Technology (JJCIT)*, *3*(2), pp.110-130.

Work Done	In this article, they outlined a novel method for securing data communication systems that combines steganography and cryptography. The Modified Jamal Encryption Algorithm (MJEA), a symmetric (64-bit) block encryption algorithm with a (120-bit) key, was the cryptography algorithm used in this paper. They created an improved version of the Least Significant Bit (LSB) algorithm with a (128-bit) steg-key for steganography. The impressibility test, embedding capacity test, and security test are just a few of the experimental tests that have been used to gauge how well the proposed technique performs. The suggested method was used on several 24-bit coloured PNG cover images for this purpose.
Techniques Used	In order to provide secure data transmission over insecure channels, they proposed a hybrid security system in this study that combines cryptography and steganography techniques. Through a variety of experiments, MJEA's performance was assessed in [37]-[38]. Through a number of simulation tests, the MJEA plain text encryption algorithm has been thoroughly examined. When the algorithm is run for at least four rounds, the plaintext and key are completely scrambled.
Observation	The strength of the suggested algorithm in securing the transfer of data over insecure channels to defend it against any attack was demonstrated by all experimental results. Furthermore, when compared to other algorithms in terms of PSNR and embedding capacity, the simulation results demonstrate our proposed algorithm's superiority.

Paper Title	**Hybrid cryptography and steganography method to embed encrypted text message within image**
Citation	Jassim, K.N., Nsaif, A.K., Nseaf, A.K., Priambodo, B., Naf'an, E., Masril, M., Handriani, I. and Putra, Z.P., 2019, December. Hybrid cryptography and steganography method to embed encrypted text message within image. In *Journal of Physics: Conference Series* (Vol. 1339, No. 1, p. 012061). IOP Publishing.
Work Done	The primary goal of this research is to increase the level of security provided by cryptography by using a supporting technique called steganography. The process of hiding data or information in media files like audio, video, and image files is called steganography. The four stages that make up this paper's methodology are as follows: (1) use the RSA algorithm to encrypt the original texts; (2) conceal the encrypted texts in image files; (3) extract the encrypted texts from image files; and (4) use the RSA algorithm's decryption key to decrypt the original texts. It is anticipated to raise the level of security for text data transferred online.
Techniques Used	This paper's main focus is on using cryptography and steganography to protect text data. The RSA Algorithm will be used to encrypt the data. On the other hand, image files with the (.bmp) extension will conceal the encrypted data. The methodology is divided into four main phases, which are as follows: (1) Create the encryption keys and use RSA to encrypt the text data. (2) Utilize image files to conceal the encrypted data. (3) Take the encrypted information out of the image files. (4) Using the decryption key, decrypt the text data.
Observation	The PSNR between the steganography image and the original image is 83.2591. The LSB method has thus been successfully applied, and results have been obtained. The results show that in LSB-based steganography, PSNR is high and MSE is low.

Paper Title	Steganography Techniques –A Review Paper
Citation	Jasleen Kour,Deepankar Verma, Steganography Techniques –A Review Paper, International Journal of Emerging Research in Management &Technology
Work Done	Et al. examined a wide range of papers on steganography methods.These studies are adequate and have a broad potential application. They discovered through reading these publications that the majority of the steganography work was done in 2012 and 2013. These days, the most used steganography method is called LSB. Some scholars have utilised the methods including water marking, distortion, spatial, ISB, and MSB were used in their work and offered a reliable method of securely transmitting information.
Techniques Used	The many security and data-hiding methods, such as LSB, ISB, MLSB, etc., that are used to implement a steganography are reviewed in this work.
Observation	The many data-hiding and security methods LSB, ISB, and MLSB are utilised to execute steganography .In further research they are going to use more advance schemes like steganography with some hybrid cryptographic algorithm for enhancing the data security.

Paper Title	Information Hiding using Steganography
Citation	Ritu Sindhu, Pragati Singh, Information Hiding using Steganography, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958 (Online)
Work Done	The paper provides a summary of various steganography techniques, methodologies, standards, benefits, drawbacks, and major types. It also explains a methodology that may use any form of image file without converting it to bitmap and that uses the most memory space possible to conceal data in images.
Techniques Used	Encryption,Decryption technique in stegnography shown in the paper which can take a file and image convert it into a file having a BMP image and during decryption convert it into a file adn image.
Observation	This study also makes an effort to determine which Steganography approaches are more effective, what those techniques' needs are, and which applications will work best with each Steganography methodology.

Paper Title	Wavelet transform based steganography technique to hide audio signals in image.
Citation	Hemalatha S , U. Dinesh Acharya , Renuka A, Wavelet transform based steganography technique to hide audio signals in image, e CC BY-NC-ND license.

Work Done	Et al. proposed a high-capacity, safe, and reliable image steganography technique.This is a good approach to deliver audio files without exposing their presence because it provides good values for all the criteria.The performance against some of the attacks is also good.It's important to evaluate the method against several types of attacks, such as histogram equalisation, cropping, occlusion, translation, etc
Techniques Used	As audio files contain numerous samples, even for brief periods of time, the cover image must be quite huge. Due to ample concealing space, colour photos are appropriate. The YCbCr technique is utilised because it is safer than the RGB approach. It changes the cover image to YCbCr. Then, using IWT, the Cb, Cr, and hidden audio signal are changed. The second and third bit planes of the high frequency coefficients of the Cb and Cr include the estimated coefficients of the secret audio stream.
Observation	According to the experimental findings, the hidden audio can typically be retrieved without considerable distortion.

Paper Title	Edge-based image steganography
Citation	Saiful Islam , Mangat R Modi and Phalguni Gupta, Edge-based image steganography,
Work Done	Et al. have put forward an innovative method for steganography in grayscale photographs has been put forth in this study. The cover image's edges, which are dynamically chosen based on the message's length, have data that is hidden

	from view. Compared to the current edge-based strategies, the suggested method can withstand visual, structural, and non-structural attacks better.
Techniques Used	Edge based image steganography technique where edges in the cover image have been used to embed messages. The amount of data that needs to be incorporated has a significant impact on the edges that are chosen; the more data that needs to be included, the more weaker edges are used. The proposed method works better than, or at least on par with, state-of-the-art steganography approaches while offering a higher embedding capacity, according to experimental data.
Observation	If one employs syndrome coding to lessen the amount of distortion brought on by embedding, the proposed technique should perform better.

Paper Title	A Novel Steganography Method for Image Based on Huffman Encoding
Citation	RigDas,Themrichon Tuithung, A Novel Steganography Method for Image Based on Huffman Encoding
Work Done	Et al. provide a brand-new Huffman Encoding-based image steganography technique. The algorithm is superior than other algorithms already in use and enhances the security and quality of the stego picture.

Techniques Used	To extract the hidden image or message, the decoder just needs to be aware of the extraction algorithm. The secret image is protected against theft and destruction by any unauthorised users thanks to Huffman encoding; as a result, the suggested solution may be more resistant to brute force attacks.
Observation	The outcome of the trial demonstrates the algorithm's great capacity and strong invisibility. Peak Signal to Noise Ratio (PSNR) of stego image with cover image also exhibits improved results in comparison to other steganography techniques currently in use.

Paper Title	Information Hiding in Images Using Steganography Techniques
Citation	Ramadhan Mstafa , Christian Bach, Information Hiding in Images Using Steganography Techniques, Norwich University March 14-16, 2013
Work Done	In this paper, Et al. review some techniques of steganography and digital watermarking in both spatial and frequency domains. Since these issues first surfaced, numerous approaches have been developed. Steganography is a practical method for safeguarding information transmitted over the internet. One of the often used steganographic applications is digital watermarking. When transmitting data, users might use an invisible watermark to conceal sensitive information within a picture.

Techniques Used	Steganography is a practical method for safeguarding information transmitted over the internet. One of the often used steganographic applications is digital watermarking. When transmitting data, users might use an invisible watermark to conceal sensitive information within a picture.
Observation	This alteration does not affect the intensity of the color.

Paper Title	Image Steganography Techniques: An Overview
Citation	Nagham Hamid,Osamah M. Al-Qershi,R. Badlishah Ahmad,Abid Yahya, Image Steganography Techniques: An Overview
Work Done	Et al. examined the most common steganographic methods for lossy and lossless picture formats, including JPEG and BMP. The taxonomy of existing steganographic approaches for image files has been described because the focus of this paper is on the usage of an image file as a carrier. These methods are examined and discussed not only in terms of their capacity to conceal data in image files but also in terms of how much data can be concealed and their resistance to various image processing assaults.
Techniques Used	Statistical Methods **,**Distortion Techniques,File Embedding, Pallet Embedding
Observation	The results are described in terms of a taxonomy that centres on the three main steganographic methods for concealing data in

	image files. These methods include those that alter the image's spatial properties, its transform properties, and its file formatting.

Paper Title	Digital Image Security: Fusion of Encryption, Steganography and Watermarking
Citation	Ashfaque Ahmed Memon,Mirza Adnan Baig,Riaz Ahmed Shaikh,Mirza Abdur Razzaq, Digital Image Security: Fusion of Encryption, Steganography and Watermarking
Work Done	Et al. proposed hybrid security method for the protection of digital images. It combines three security measures: steganography, encryption, and watermarking. The proposed approach basically included three phases.
Techniques Used	In the first phase encryption was performed using XOR to the right rotate pixel bits.The second stage of steganography then involved replacing bits of the encrypted image with LSBs from the cover image. The third step concluded with time and frequency domain watermarking.
Observation	The proposed approach is efficient, simpler and secured; it provides significant security against threats and attacks. The experimental findings from the proposed method were encouraging; the achieved PSNR of 55.4993 dB demonstrated the method's high efficiency and security. Secret key will also be used in steganography in upcoming projects.

Paper Title	Data Hiding with Deep Learning: A Survey Unifying Digital Watermarking and Steganography
Citation	QI WU, MINHUI XUE, CONGBO MA, HU WANG, WENDY LA, OLIVIA BYRNES, Data Hiding with Deep Learning: A Survey Unifying Digital Watermarking and Steganography
Work Done	Et al. compared current state-of-the-art methodologies categorised in terms of network design and model performance, and provided an overview of deep learning strategies for data concealment, including both watermarking and steganography. The survey examined objective functions and evaluation metrics for measuring model performance before looking at potential future lines of inquiry for this area of study. This survey summarises recent developments in deep learning techniques for data hiding for the purposes of watermarking and steganography, categorising them based on model architectures and noise injection methods.
Techniques Used	Deepfake Detection and Identification, Malware using Steganography, Watermarking for Launching Backdoor Attacks, Watermarking for Protecting Machine Learning Models, Mitigating Watermark Removal Attacks, Text Watermarking for Combating Misinformation
Observation	Deep learning-based solutions for data hiding will probably outperform any classical algorithms in all media and considerably increase digital information security as technology advance and applications proliferate to various types of media.

Paper Title	An Information-Theoretic Approach to Steganography and Watermarking
Citation	Thomas Mittelholzer, An Information-Theoretic Approach to Steganography and Watermarking
Work Done	A model for a stego system was presented, which gives a novel characterization of the two critical components the embedding process and the attacker's alteration of a stego message are two crucial components that are characterised in a novel way by a model for a stego system that was recently provided. The maximum distortion between the cover message, the stego message, and the modified stego message is the basis for the definition of the two components.
Techniques Used	In a steganographic technique, certain cover data is used to conceal a secret message V.The stego encoder embeds the secret message by fusing the secret message V into the cover data U, which is made up of a string of random variables, based on some secret key K. The stego encoder fk(.,.) generates the stego message X = fk(U, V) for each key value k, which is once more a series of random variables.
Observation	Thomas with the help of this model, one may approach steganography from an information-theoretic perspective and express the two fundamental problems of secrecy and robustness in terms of mutual information.

Paper Title	Steganography and Its Applications in Security
Citation	Ronak Doshi, Pratik Jain, Lalit Gupta, Steganography and Its Applications in Security
Work Done	In this study, various methods for encoding data in text, image, and audio/video signals as cover media are presented. I've given a succinct summary of a very dynamic and intriguing subject of computer security. Many in the security industry are concerned about this technology because of the potential harm it could cause to both the public and private sectors of industry. This technology will develop significantly and into the mainstream as pcs become more powerful. Numerous steganography programmes are currently in existence and may be applied to text, audio, and image files. The federal government and numerous private businesses are looking into the best techniques to identify steganography in files. Steganalysis will be adopted as a common security tool as it develops.
Techniques Used	Steganalysis is a process in which a steganalyzer cracks the cover object to get the hidden data. So, whatever be the technique will be developed in future, degree of security related with that has to be kept in mind. It is hoped that Dual Steganography, Steganography along with Cryptography may be some of the future solution for this above mentioned problem.
Observation	The research to device strong steganographic and steganalysis technique is a continuous process.

Paper Title	On the Limits of Steganography
Citation	Ross J. Anderson and Fabien A. P. Petitcolas, On the Limits of Steganography
Work Done	Et al have explored the limits of steganographic theory and practice.They began by discussing a variety of both traditional and contemporary methodologies, along with some (new) criticisms of them, and we then spoke about many potential trajectories for a theory on the matter. With the same force as Shannon's idea of perfect secrecy, we identified the obstacles to a theory of "perfect covertness." The "selection channel"—the bandwidth of the stego key—and considerations of entropy, however, provide us some mathematical power, which is why we recommend embedding information in parity checks rather than the actual data.
Techniques Used	Public key steganography until recently, it was generally assumed that, in the presence of a capable motivated opponent, steganography required the pre-existence of a shared secret, so that the two communicating parties could decide which bits to tweak.
Observation	This approach gives improved efficiency, and also allows us to do public key steganography. Finally, they shown that public key steganography may sometimes be possible in the presence of an active warden.

Paper Title	Pros and Cons of Cryptography, Steganography and Perturbation techniques
Citation	Haripriya Rout , Brojo Kishore Mishra, Pros and Cons of Cryptography, Steganography and Perturbation techniques, IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834,p- ISSN: 2278-8735.
Work Done	Here they have done a comparative study on cryptography, steganography and perturbation technique with pros and cons of each. Mainly, there are three ways we can protect our data. The first is cryptography, where the message's substance is concealed by encoding it; the second is steganography, where the message is embedded in another medium; and the third is perturbation technique, which modifies the actual data so that its true meaning is concealed.
Techniques Used	· Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions. · Steganography's major objective is to ensure secure communication that is absolutely undetected in order to avoid raising questions about the transfer of secret data. It's not to stop people from finding out the secret knowledge; rather, it's to stop people from believing that information even exists. A steganography technique fails if it leads someone to question the carrier media.

Observation	The key to data encryption within a company is strategic planning because there are numerous factors, both positive and negative, to take into account. Without careful preparation, managing data encryption can quickly become difficult for the IT administrator and difficult for the end users.

Paper Title	A Comparative Study of Steganography & Cryptography
Citation	Pranali R. Ekatpure, Rutuja N Benkar, A Comparative Study of Steganography & Cryptography, International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064
Work Done	Et al. after comparing states that it is difficult to state with certainty that Steganography can be used as an alternative to cryptography after an unsatisfactory comparison. Although cryptography provides services that are more secure, there are certain drawbacks. This does not, however, establish categorically that Steganography cannot be used in place of cryptography. Steganography and cryptography are combined in this way to address all security concerns.
Techniques Used	Text Steganography, Image Steganography, Audio Steganography, Video Steganography, Symmetric Key Cryptography, Asymmetric Key Cryptography
Observation	Combination of cryptography and Steganography is used so all security purpose are solved

Paper Title	Combination of Steganography and Cryptography: A short Survey
Citation	Mustafa Sabah Taha et al 2019 IOP Conf. Ser.: Mater. Sci. Eng. 518 052003
Work Done	Et al. after conducting a comparison study between the science of cryptography and steganography, the authors cannot guarantee that steganography can be used as a substitute for cryptography. Utilizing just one of these methods will leave the system open to attack. The act of secret writing through the encoding and decoding of encoded messages is known as cryptography, whereas steganography refers to the ways of concealing a secret message into a cover message in such a way that its existence is completely hidden.
Techniques Used	The data may be compromised, distorted, or even deployed for future attacks by attacker. Exploiting the benefits of cryptography and steganographic techniques to create a hybrid system that can be stronger than the individual strengths of the component approaches would be the ideal way to solve these difficulties. By combining these approaches, you may ensure that your secret information is more secure and that your transmission of sensitive information through public channels is secure and reliable.
Observation	The combination of Steganography and Cryptography give more security and robustness.

Paper Title	**Image Cryptography Using RSA Algorithm in Network Security**
Work Done	http://ijcset.net/docs/Volumes/volume5issue9/ijcset2015050902.pdf There aren't many algorithms, which makes computations difficult and makes it challenging to crack a code and uncover the original content. In this instance, the RSA method is utilised to picture files to improve communication security for data transmission. To move data from one location to another, encryption and decryption are performed on an image file using a key generation process.
Techniques and Keywords	1. RSA Algorithm, 2. Images 3. Symmetric Key 4. Asymmetric Key 5. Key Generation 6. Prime Numbers 7. Hex Code

Paper Title	**Digital Image Encryption Based on RSA Algorithm**
Work Done	https://www.researchgate.net/profile/Abbas-Wahab/publication/330667343_Modified_Mathematical_Method_to_Improve_RSA_Image_Cryptosystem_Algorithm/links/5c7cc028299

	bf1268d365ac4/Modified-Mathematical-Method-to-Improve-RSA-Image-Cryptosystem-Algorithm.pdf It begins by concentrating just on the issue of secret communication. The term also describes cryptography as an artistic endeavour. Cryptography was, in fact, an art form up until the 20th century (and perhaps even until the latter half of that century). This understanding of cryptography drastically changed in the late 20th century. A thorough theory was developed, allowing for the scientifically rigorous study of cryptography. In addition, cryptography today covers a wide range of applications outside secret communication, such as message authentication, digital signatures, authentication protocols, protocols for sharing secret keys, electronic auctions and elections, and digital money. Throughout the lengthy history of secret communications, the inventions of public key cryptography by Diffie and Hellman in 1976 and the RSA public key cryptosystem that followed by Rivest, Shamir, and Adleman in 1978 are defining moments. The significance of public key cryptosystems and the digital signature techniques they are connected with in today's computer and Internet world cannot be overstated.
Techniques and Keywords	1. Cryptography 2. Information security 3. Image Encryption 4. RSA 5. DES 6. Blowfish

Paper Title	**A security enhanced robust audio steganography algorithm for image hiding using sample comparison in discrete wavelet transform domain and RSA**

	encryption
Work Done	https://link.springer.com/article/10.1007/s11042-016-4113-8 The cover audio is divided into numerous multi-band sub-bands, and then selected coefficients of details are altered by a threshold value depending on the embedding cypher image bit in this paper's proposed efficient steganography system based on sample comparison in the DWT domain. This method uses an original picture component to encrypt it using RSA, after which cypher bits are inserted in the audio signal's detail components in accordance with a predetermined threshold value. The resilience of the suggested approach is demonstrated by simulation results that show the performance of the algorithm has been extensively estimated against attacks.

Paper Title	**An asymmetric image encryption scheme based on hash SHA-3, RSA and compressive sensing**
Work Done	https://www-sciencedirect-com.egateway.vit.ac.in/science/article/pii/S0030402622009627 Initially, a random matrix is created, and then the plain image is added to it using a modular operation to create a preprocessed image. The preprocessed image's hash values are next calculated using the third-generation secure hash technique (SHA-3), and they are then added together to provide three plaintext keys. Three ciphertext keys can be obtained in the appropriate order using Rivest-Shamir-Adleman (RSA). Second, a brand-new mathematical transformation model (MTM) is created to convert all keys into chaotic system's beginning values. Keystream is then computed in accordance with that. Lastly, random sequences are employed to further confuse the plain image after it has been compressed using compressive sensing (CS). The confused image was then subjected to discrete wavelet transformation (DWT), which produced four components with high and low frequencies. The low frequency components are once more confused using chaotic sequences before being once more integrated into a matrix. To obtain a middle cypher picture, perform inverse DWT (IDWT) after that (MCI). The final cypher picture is produced by another random matrix created by chaotic sequences, and it is then obtained by performing a modular addition operation to the MCI once more.
Techniques	1. Image encryption 2. Chaotic system

and Keywords	3. Asymmetric encryption 4. SHA-3 5. Compressive sensing

Paper Title	**An optical image compression and encryption scheme based on compressive sensing and RSA algorithm**
Work Done	https://www-sciencedirect-com.egateway.vit.ac.in/science/article/pii/S0143816618316415 An optical image compression and encryption strategy based on compressive sensing and the RSA public-key cryptography algorithm has been presented to increase the security of image encryption systems. The optical compressive imaging system is used to sample the original image in this scheme. The Walsh-Hadamard transform and a measurement matrix are used in the encryption process to imitate an optical compressive imaging system and measure the original image, thus reducing duplicate information. The resulting image's pixel coordinates are then mixed up using a pseudorandom sequence created by a chaotic cascade in one dimension (1D).
Techniques and Keywords	1. Compressive sensing 2. Optical image encryption 3. DNA Sequence operations 4. RSA Algorithm 5. Chaotic system

Paper Title	**RSA-based Encryption Algorithm for Digital Images**
Work Done	https://ieeexplore-ieee-org.egateway.vit.ac.in/document/10010627 Since the RSA cryptosystem is a reliable and well-known asymmetric encryption system, a digital picture encryption algorithm based on it is proposed in this paper. As opposed to encrypting each pixel individually, the suggested approach divides the image into blocks of 22 size. This enhances encryption and turns each block into a single vector after that. A single binary number is created from the vector's elements after they have been translated to binary. The binary number is then translated to decimal to make it work with the RSA method. The suggested approach restores the original image without sacrificing any data or information; it is lossless. The recommended approach is then tested on numerous photos in the MATLAB environment.

Paper Title	**Image Encryption Method Using Differential Expansion Technique, AES and RSA Algorithm.**
Work Done	https://ieeexplore-ieee-org.egateway.vit.ac.in/document/8985665 Using conventional encryption techniques now makes it harder to provide security. It is suggested to combine two conventional encryption techniques to avoid this problem. Then, embed an encrypted confidential key into the hidden image using the Differential Expansion approach. One scenario is that the malicious individual is unaware of the cypher text and the enciphered key. The likelihood of an attack is very low. On the other side, if the hacker is aware of the cypher key, he can obtain the plaintext image using the private key. As compared to other current algorithms, the suggested approach is strong and offers superior security. It will be put into practise in MATLAB.
Techniques	

and Keywords	1. Substitute Bytes 2. Shitfrows 3. Addroundkey 4. Mix Columns

Paper Title	**The design and implementation of hybrid RSA algorithm using a novel chaos based RNG**
Work Done	https://www-sciencedirect-com.egateway.vit.ac.in/science/article/pii/S0960077917303818 This study begins with the creation of a brand-new chaotic system with high dynamic properties before moving on to the implementation and analysis of the circuit. With the aid of the newly created chaotic system, a chaos-based random number generator is created, and NIST and FIPS tests are done. RNG and RSA algorithms are combined in the creation of the chaos-based hybrid RSA (CRSA) encryption algorithm. The technique is used to encrypt text and images, and security evaluations of various applications are performed. The outcomes of security evaluations are contrasted with the traditional RSA algorithm. In security tests, it was found that the developed CRSA algorithm performed better than the RSA method.

System Design

User Interface: The UI of your application should allow users to upload a file to be secured as well as download the secured file.

Flask Microservice: You must set up a Flask microservice to handle UI requests. This microservice should expose a file upload endpoint that returns the secured file.

Symmetric Key Cryptography: To encrypt the uploaded file, your application should use a symmetric key cryptography algorithm such as AES or DES. The encryption key should be generated randomly for each upload and never shared with anyone.

Modified LSB Steganography: After encrypting the file, use the modified LSB steganography algorithm to embed the encrypted data into an image or audio file. In order to encode the encrypted data, the modified LSB algorithm will modify the least significant bits of the pixels in the image. The encrypted data will be virtually invisible to the human eye.

Download: After the modified LSB algorithm has encoded the encrypted data into the image or audio file, the user can download the resulting file. When the user wants to view or listen to the encrypted file, they can use your application to extract the encrypted data from the image and then decrypt it with the same key that was used to encrypt it.

Objective 1 AES Algorithm

1. Key Expansion: To create a key schedule, the AES algorithm begins by expanding the initial encryption key. The key schedule is used to generate round keys for each round of the encryption process.

2. The plaintext is initially XORed with the first round key. Following this, there are 9 rounds of transformations that include SubBytes, ShiftRows, MixColumns, and AddRoundKey operations.

3. The final round is similar to the previous rounds, but it excludes the MixColumns operation.

4. Inverse Cypher: The inverse cypher is used to decrypt the ciphertext. In reverse order, the inverse cypher consists of the InvSubBytes, InvShiftRows, InvMixColumns, and AddRoundKey operations.

5. AES requires that the plaintext be a multiple of 16 bytes in length. If the plaintext is not already a multiple of 16 bytes, it must be padded with more bytes.

6. The AES algorithm can be used in a variety of block cypher modes, including ECB, CBC, CFB, OFB, and CTR. The mode used determines how the plaintext is broken down into blocks and how the ciphertext is generated.

7. Initialization Vector: To ensure that the same plaintext does not always produce the same ciphertext, some block cypher modes, such as CBC and CFB, require the use of an initialization vector (IV). Before encryption, the IV is XORed with the first plaintext block, and the resulting ciphertext block is then used as the IV for the next block.

Advantages

AES is widely recognised as a highly secure encryption algorithm. It has been thoroughly examined by cryptographers and extensively tested in the real world.

AES is designed to be quick and efficient, making it suitable for a wide range of applications. It is supported by most modern processors and operating systems and can be implemented in hardware or software.

AES is a versatile algorithm that can be used for a wide range of applications, including file encryption, network encryption, and disc encryption.

Disadvantages

AES encryption can be resource intensive, especially when dealing with large amounts of data. This can result in slower performance and longer processing times.

AES requires proper key management to ensure that encryption keys are generated, stored, and distributed securely. The encrypted data may be jeopardised if the keys are compromised or lost.
Vulnerable to Side-Channel Attacks: A side-channel attack is a type of attack that exploits vulnerabilities in an encryption system's physical implementation, such as timing, power consumption, or electromagnetic radiation. While AES is resistant to many types of side-channel attacks, it is not entirely immune to them all.

Objective 2 DES Algorithm:

1)Key generation: To create 16 subkeys, each 48 bits long, the 56-bit encryption key is put through a sequence of changes known as the key schedule.

2)Initial permutation (IP) table: The initial permutation (IP) table is used to permute the 64-bit plaintext block.

3)Feistel network: L0 and R0 are the two 32-bit halves of the permuted plaintext. Following that, these two parts go through 16 iterations—referred to as rounds—in total. The Feistel function is applied to the right half in each round, and the outcome is then XORed with the left half. The new right half is created as a result of the XOR operation, and the previous right half is transformed into the new left half.

4)Substitution is one of the operations that make up the Feistel function. Each round's 48-bit subkey is merged with the plaintext's 32-bit right half before being split into eight 6-bit blocks. Eight substitution boxes (S-boxes) are used to convert each 6-bit block into a 4-bit block.

5)The output of the Feistel function goes through additional permutation after substitution, known as the permutation or P-box.

6)Inverse initial permutation (IP-1) is the final permutation used to the resulting 64-bit block after the 16 rounds are complete in order to create the ciphertext.

7)With the exception of using the subkeys in the opposite order, the decryption procedure is the same as the encryption procedure.

Advantages

Speed: The DES encryption method is rather speedy, which makes it perfect for applications that need swift encryption and decoding.

Simpleness: DES is an easy-to-implement encryption technique that is perfect for applications that don't need the maximum level of security.

Widespread adoption: DES is a well-liked encryption technique that may be used in a number of applications because it has been widely accepted and supported by numerous software and hardware suppliers.

Due to its extensive use, DES may be used to encrypt and decrypt data on a variety of devices and operating systems.

Robustness: Although newer encryption algorithms have exceeded DES in terms of security, DES is still a robust encryption technique that may offer a respectable level of security for many applications.

Disadvantages

Key length: The fixed key length for DES is 56 bits, which is now regarded as being insufficient for modern assaults. As a result, it may be subject to brute-force attacks, in which an attacker tries every key combination until they locate the right one.

Attacks: It has been established that DES is susceptible to a number of attacks, including brute-force and differential cryptanalysis attacks. The encryption can be defeated using these approaches, allowing the original data to be seen.

Limited scalability: DES cannot readily be modified to support larger or more complicated systems because it is not scalable. Because of this, it is less appropriate for contemporary applications that need scalable encryption techniques.

Limited adaptability: Because DES is a fixed encryption method, it is difficult to adapt it to a particular application's unique requirements. This limits its adaptability to various situations and versatility.

Objective 3: RSA Algorithm

Step 1: Generate the RSA modulus

The initial procedure begins with selection of two prime numbers namely p and q, and then calculating their product N, as shown −

N=p*q
Here, let N be the specified large number.

Step 2: Derived Number (e)
Consider number e as a derived number which should be greater than 1 and less than (p-1) and (q-1). The primary condition will be that there should be no common factor of (p-1) and (q-1) except 1

Step 3: Public key
The specified pair of numbers n and e forms the RSA public key and it is made public.

Step 4: Private Key
Private Key d is calculated from the numbers p, q and e. The mathematical relationship between the numbers is as follows −

$$ed = 1 \bmod (p-1)(q-1)$$

The above formula is the basic formula for Extended Euclidean Algorithm, which takes p and q as the input parameters.

Encryption Formula

Consider a sender who sends the plain text message to someone whose public key is (n,e). To encrypt the plain text message in the given scenario, use the following syntax –

$$C = Pe \bmod n$$

Advantages

1. Security: The RSA algorithm is an extremely safe way to encode and decode sensitive data. To make it challenging for outsiders to decipher the code, it makes use of the characteristics of huge prime numbers.
2. Several applications and businesses employ the RSA algorithm, including online banking, e-commerce, and secure communications.
3. Key Exchange – RSA algorithm can be used to create digital signatures, which can help to verify the authenticity of digital documents.
4. Digital Signatures - Digital signatures, which can be used to verify the legitimacy of digital documents, can be made using the RSA algorithm.
5. Speed: The RSA technique is suited for use in real-time applications since it is comparatively quick and effective.

Disadvantages

1. Difficulty - The RSA algorithm is a tough mathematical formula that some individuals may find challenging to comprehend and use.
2. Key Size – RSA algorithm requires large prime numbers as part of the encryption process. The larger the prime numbers, the more secure the encryption, but it also increases the key size and processing time.
3. Speed: The RSA algorithm can take longer to encrypt large volumes of data than other encryption techniques.
4. Vulnerability to Quantum Computing - The RSA algorithm is susceptible to assaults from quantum computers, which might possibly decrypt the data.

5. Key Management - The RSA technique necessitates the safe management of the private key, which might be difficult in some circumstances.

Objective 4 LSB Algorithm

The Least Significant Bit (LSB) algorithm is a steganographic technique for hiding data within an image by modifying the pixel values' least significant bits. The LSB algorithm's general steps are as follows:

Choose a cover image: Select an image that will be used to conceal the hidden message. The cover image should be large enough to contain the message while maintaining image quality.

Convert the secret message to binary format: Convert the secret message to binary format. This can be accomplished by employing a tool or programme capable of converting text or other file types into binary code.

Embed the message: Modify the least significant bit(s) of the pixel value for each pixel in the cover image to embed the secret message. This is accomplished by substituting the least significant bit(s) from the secret message for the least significant bit(s). The number of bits that must be modified is determined by the size of the secret message and the quality of the cover image.
Save the edited image as: Save the modified cover image with the hidden message embedded. The image can be saved in a number of file formats, including PNG and BMP.

Message extraction: Simply reverse the process to extract the message from the modified image. To retrieve the embedded secret, extract the least significant bit(s) from each pixel in the modified image.

Results

RSA, AES, and DES are all encryption algorithms, but they have different strengths and weaknesses. Here is a comparison of these algorithms:

1. RSA: RSA is an asymmetric encryption algorithm that employs separate keys for encryption and decryption. Its primary application is to secure communications and digital signatures. RSA's key characteristics include the following:
    - Security: Although RSA is considered a secure encryption algorithm, its security is dependent on the size of the key used. Longer key sizes offer more security.
    - RSA supports a wide range of key sizes, typically ranging from 1024 to 4096 bits. Longer keys provide more security but necessitate more computational resources.
    - Speed: For large amounts of data, RSA encryption and decryption can be slower than symmetric encryption algorithms like AES and DES.

2. AES is a symmetric encryption algorithm, which means that the same key is used for both encryption and decryption. Its primary application is to secure data at rest, such as files and databases. AES's key characteristics include the following:
    - AES is widely regarded as a highly secure encryption algorithm. It has been thoroughly examined by cryptographers and extensively tested in the real world.

    - AES supports various key sizes, including 128-bit, 192-bit, and 256-bit keys. Longer keys provide more security but necessitate more computational resources.

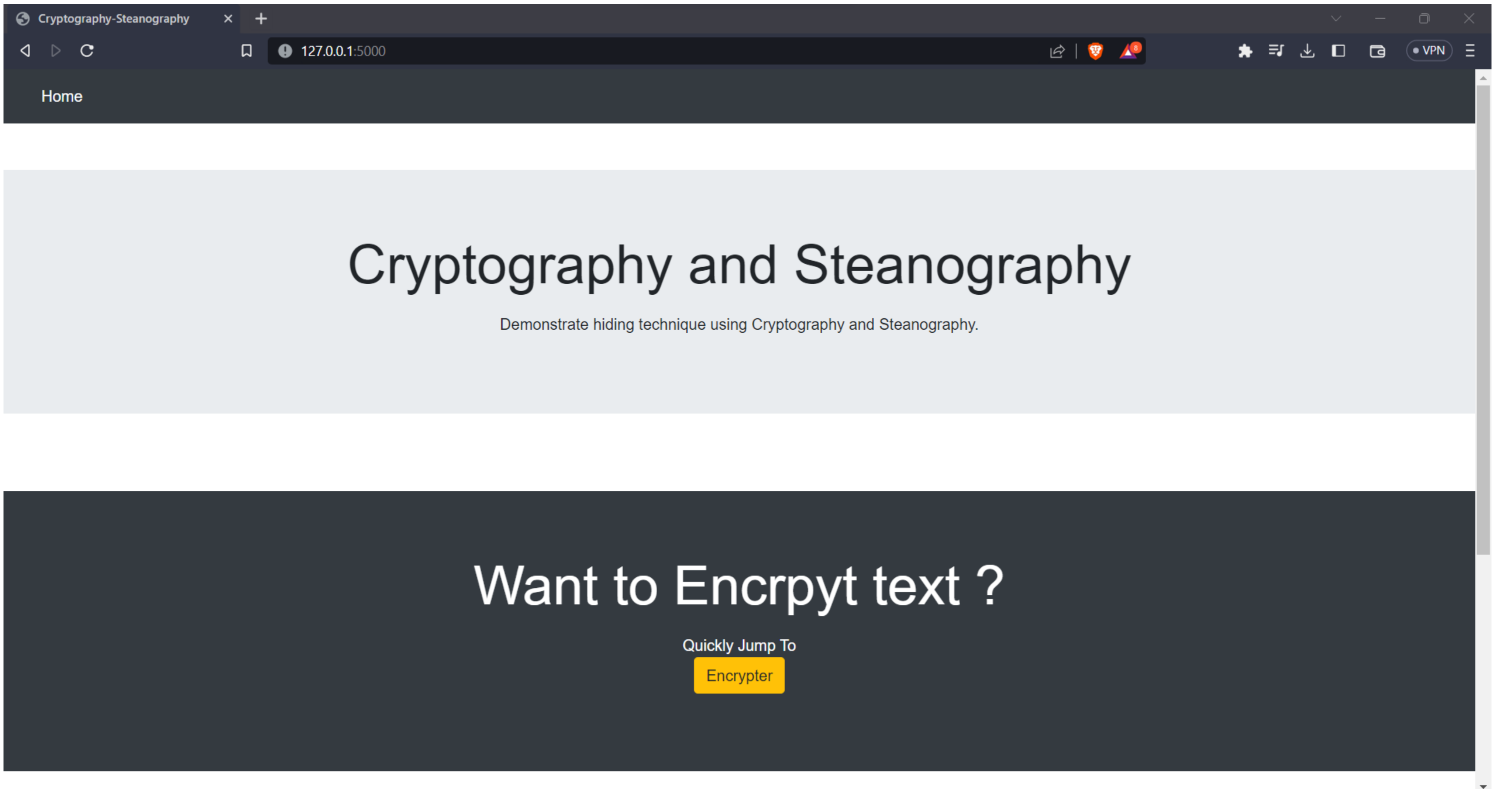
    - AES is designed to be quick and efficient, making it suitable for a wide range of applications.

3. DES: DES is a symmetric encryption algorithm invented in the 1970s. Due to security concerns, it has been largely replaced by AES. DES has the following key characteristics:
    - Security: DES is a relatively weak encryption algorithm, especially by modern standards. It is vulnerable to brute force attacks, and the key size of 56 bits is regarded as insufficient for secure encryption.

    - Key Sizes: DES employs a fixed key size of 56 bits, which is deemed inadequate for secure encryption.

    - DES is faster than AES in general, but its security flaws make it unsuitable for most modern applications.

Snapshots

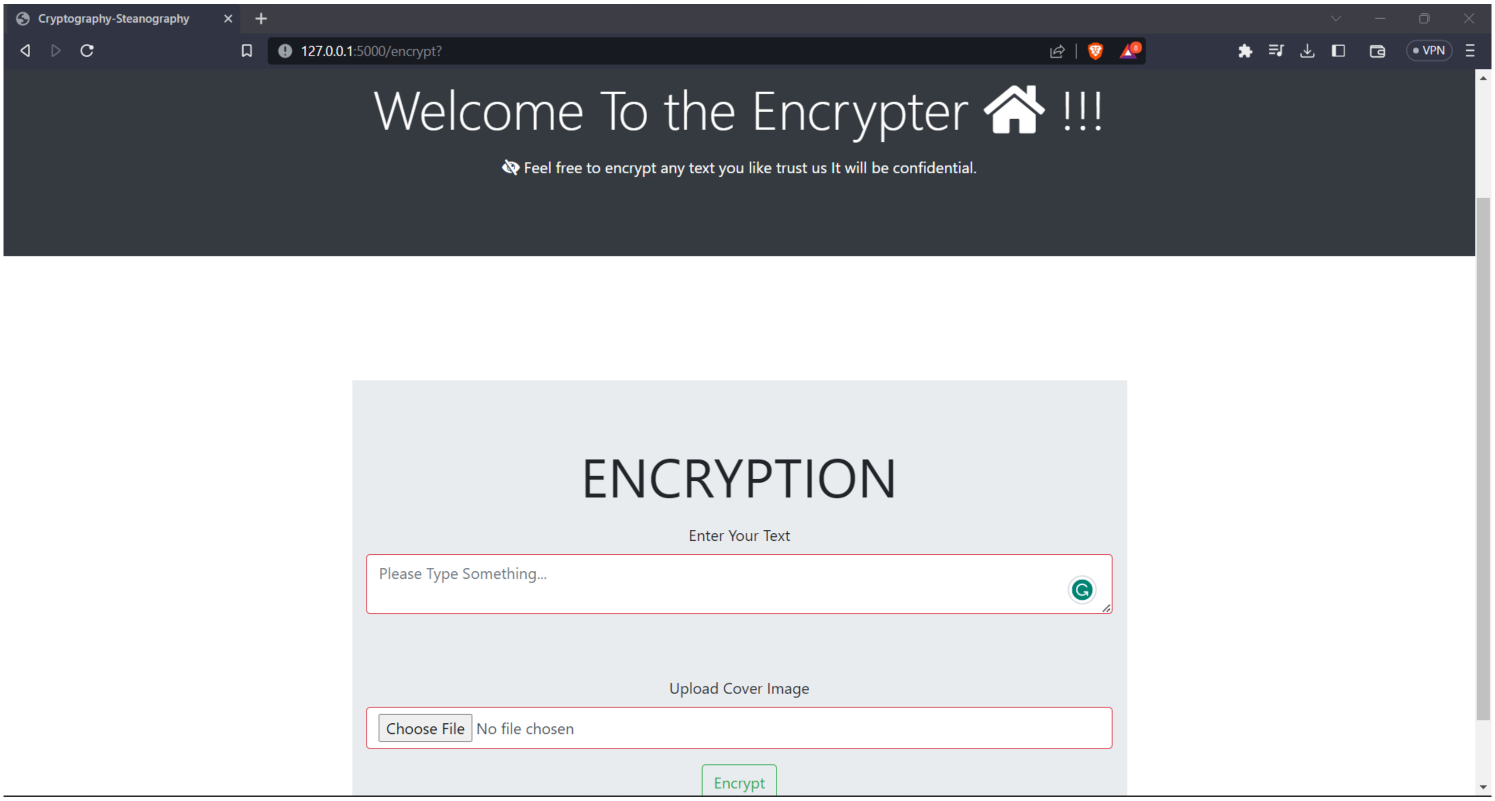


Cryptography and Steanography

Demonstrate hiding technique using Cryptography and Steanography.

Want to Encrpyt text ?

Quickly Jump To



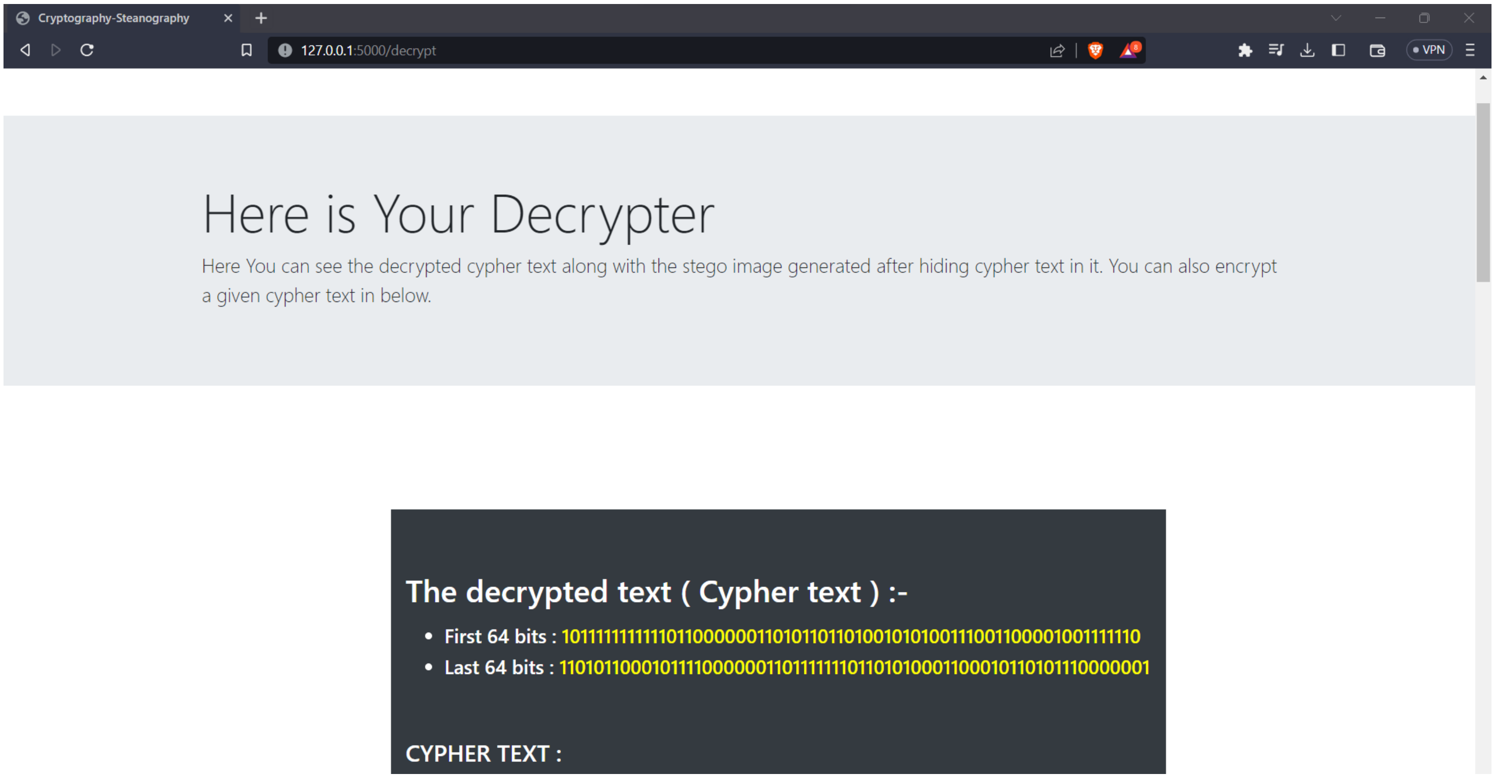
Welcome To the Encrypter !!!

Feel free to encrypt any text you like trust us It will be confidential.

ENCRYPTION

Enter Your Text

Upload Cover Image



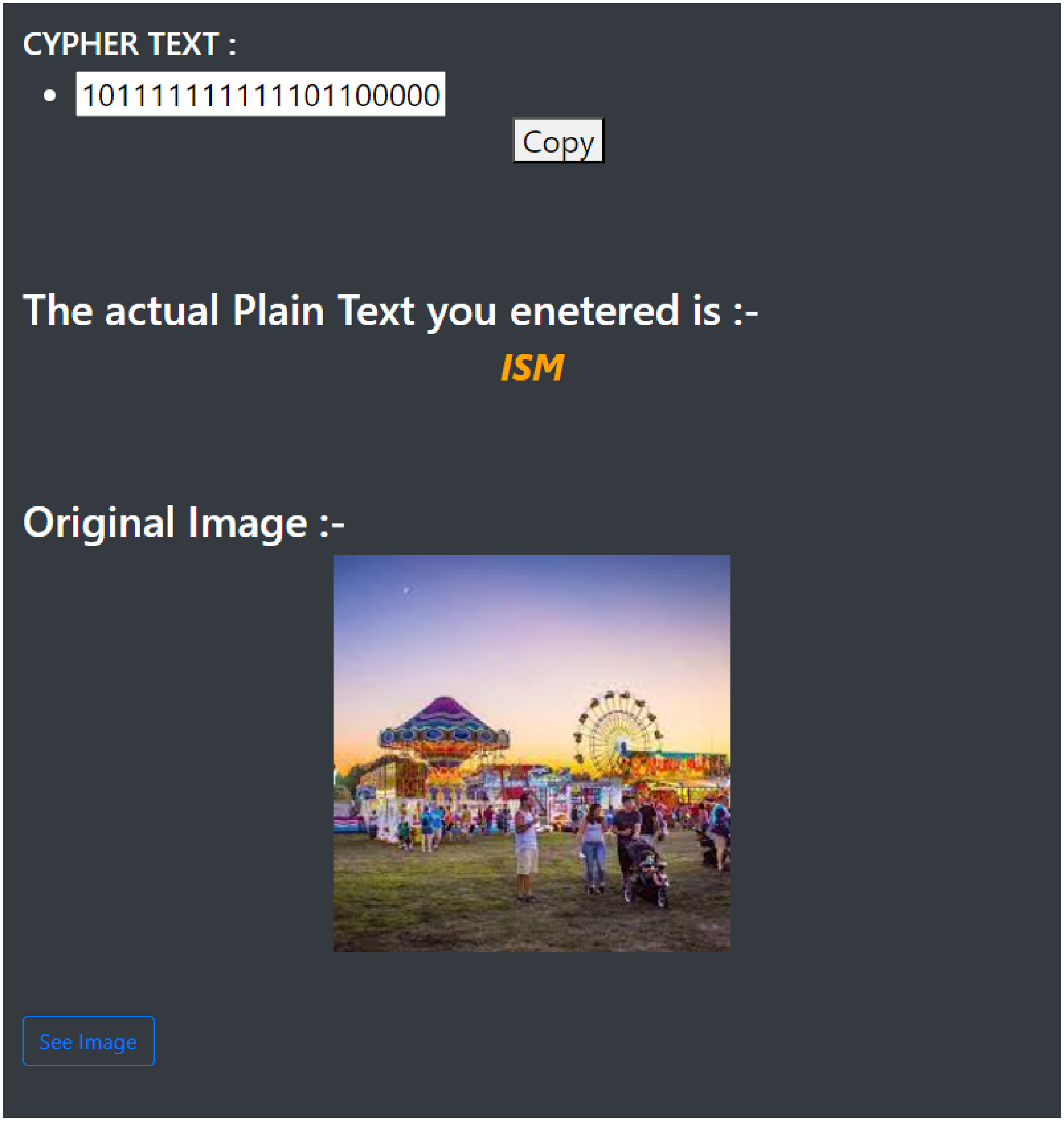
Here is Your Decrypter

Here You can see the decrypted cypher text along with the stego image generated after hiding cypher text in it. You can also encrypt a given cypher text in below.

The decrypted text (Cypher text) :-

- First 64 bits : 1011111111111011000000110101101101001010100111001100001001111110
- Last 64 bits : 1101011000101111000000110111111101101010001100010110101110000001

CYPHER TEXT :



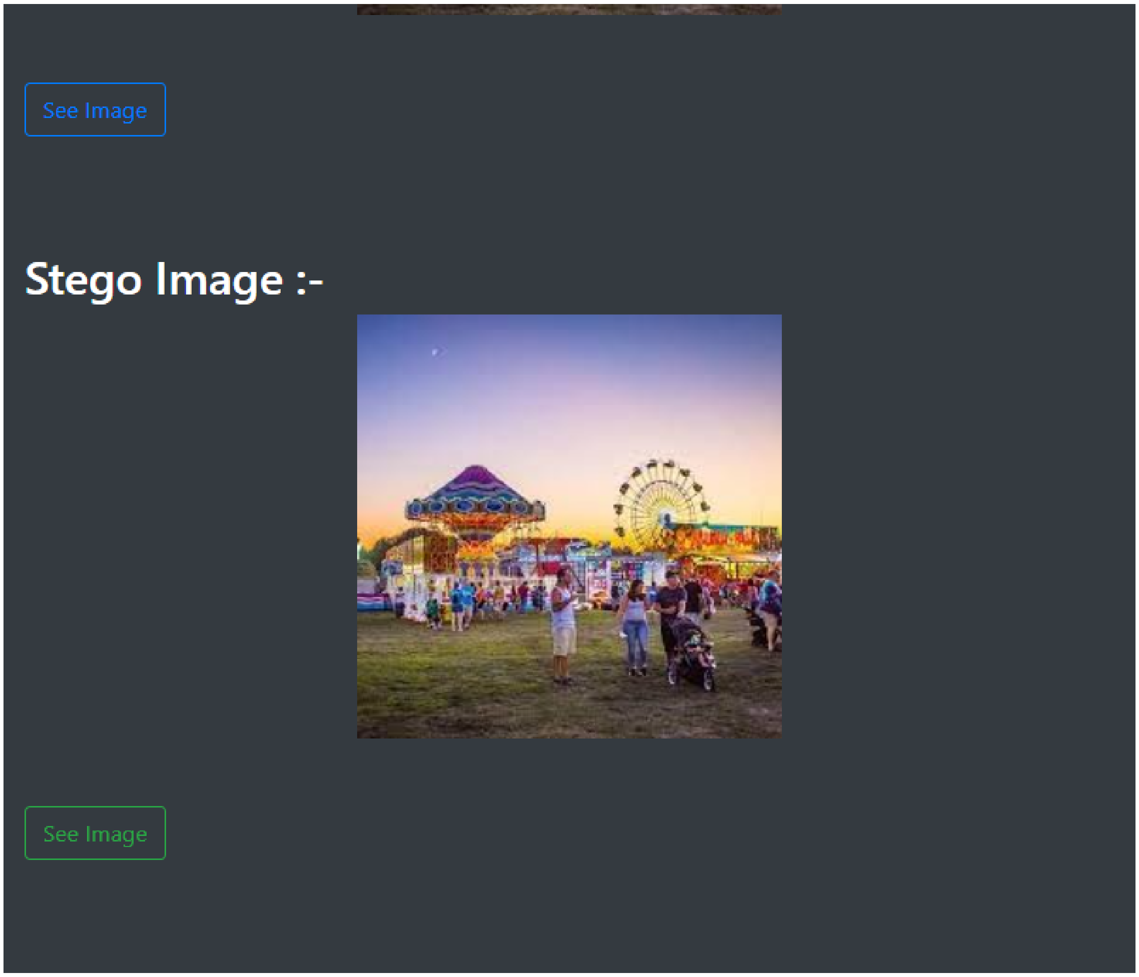
CYPHER TEXT :

- 101111111111101100000

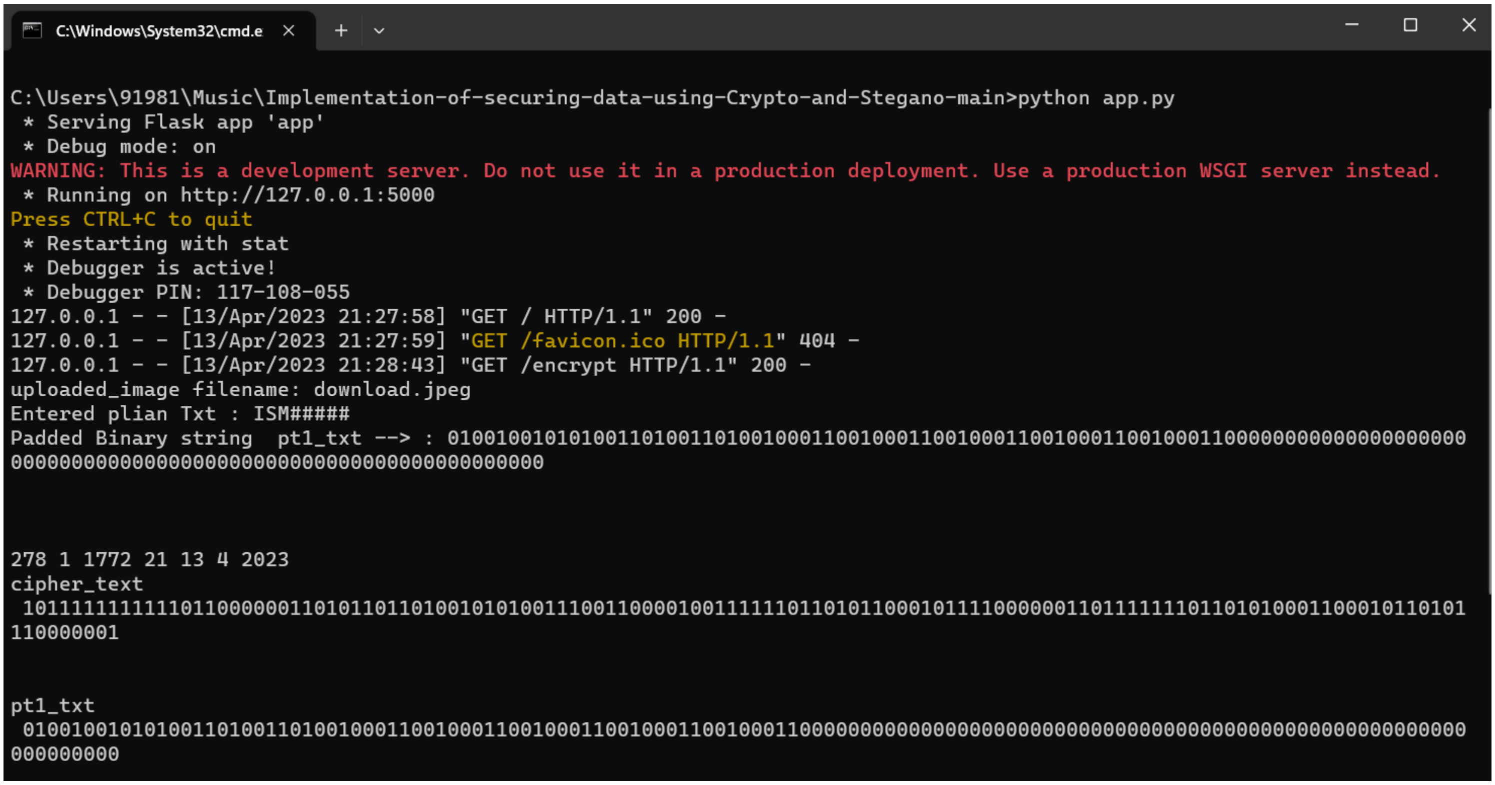
The actual Plain Text you enetered is :-

ISM

Original Image :-



Stego Image :-

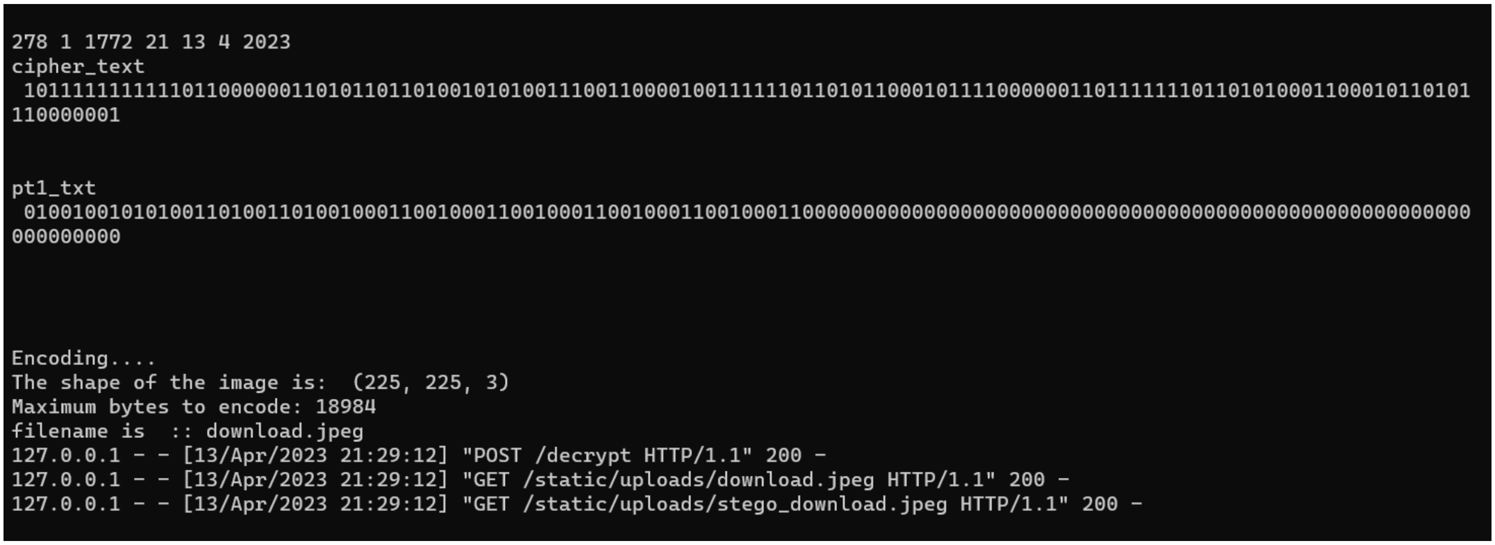


```
C:\Users\91981\Music\Implementation-of-securing-data-using-Crypto-and-Stegano-main>python app.py
 * Serving Flask app 'app'
 * Debug mode: on
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
 * Running on http://127.0.0.1:5000
Press CTRL+C to quit
 * Restarting with stat
 * Debugger is active!
 * Debugger PIN: 117-108-055
127.0.0.1 - - [13/Apr/2023 21:27:58] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [13/Apr/2023 21:27:59] "GET /favicon.ico HTTP/1.1" 404 -
127.0.0.1 - - [13/Apr/2023 21:28:43] "GET /encrypt HTTP/1.1" 200 -
uploaded_image filename: download.jpeg
Entered plian Txt : ISM#####
Padded Binary string  pt1_txt --> : 0100100101010011010011010010001100100011001000110010001100100011000000000000000000000
0000000000000000000000000000000000000000000



278 1 1772 21 13 4 2023
cipher_text
 101111111111110110000001101011011010010101001110011000010011111101101011000101111000000110111111101101010001100010110101
110000001


pt1_txt
 010010010101001101001101001000110010001100100011001000110010001100000000000000000000000000000000000000000000000000000000
000000000
```



```
278 1 1772 21 13 4 2023
cipher_text
 10111111111110110000001101011011010010101001110011000010011111101101011000101111000000110111111101101010001100010110101
110000001


pt1_txt
 01001001010100110100110100100011001000110010001100100011001000110000000000000000000000000000000000000000000000000000000
000000000




Encoding....
The shape of the image is:  (225, 225, 3)
Maximum bytes to encode: 18984
filename is  :: download.jpeg
127.0.0.1 - - [13/Apr/2023 21:29:12] "POST /decrypt HTTP/1.1" 200 -
127.0.0.1 - - [13/Apr/2023 21:29:12] "GET /static/uploads/download.jpeg HTTP/1.1" 200 -
127.0.0.1 - - [13/Apr/2023 21:29:12] "GET /static/uploads/stego_download.jpeg HTTP/1.1" 200 -
```

References

1. A. M. Qadir and N. Varol, "A Review Paper on Cryptography," 2019 7th International Symposium on Digital Forensics and Security (ISDFS), Barcelos, Portugal, 2019, pp. 1-6,
   doi: 10.1109/ISDFS.2019.8757514.

2. A Survey on Symmetric and Asymmetric Cryptography Algorithms in information Security M. A. Al-Shabi* *Department of Management Information System, College of Business Administration, Taibah University, Saudi Arabia, mshaby@taibahu.edu.sa

   DOI: 10.29322/IJSRP.X.X.2018.pXXXX

3. Muhammad Rana, Quazi Mamun, Rafiqul Islam, Lightweight cryptography in IoT networks: A survey,Future Generation Computer Systems,Volume 129,2022,Pages 77-89, ISSN 0167-739X,

   https://doi.org/10.1016/j.future.2021.11.011

4. S. Singh and V. K. Atria, "Dual layer security of data using LSB image steganography method and AES encryption algorithm, " International Journal of Signal Processing, Image Processing and Pattern Recognition, vol. 8, no. 5, pp. 259–266, 2015. DOI: http://dx.doi.org/10.14257/ijsip.2015.8.5.27
5. Dipesh G. Kamdar1, Dolly Patira2, Dr. C. H. Vithalani3 1Department of Electronics and Communication, JJ Tibrewala University, Jhunjhunu, Rajasthan, India – 333001. Department of Computer Engineering, VVP Engineering College, Rajkot, Gujarat, India - 360005 3Department of Electronics and Communication, Government Engineering College, Rajkot,Gujarat, India – 360005 International Journal of Scientific Engineering and Technology www.ijset.com, Volume No.1, Issue No.4, pg :134-138

   https://ijset.com/publication/v1/115.pdf

6. M. Panda, "Performance analysis of encryption algorithms for security," 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), Paralakhemundi, India, 2016, pp. 278-284, doi: 10.1109/SCOPES.2016.7955835.
7. K. Logunleko, O. Adeniji, and A. Logunleko, “A comparative study ofsymmetric cryptography mechanism on des aes and eb64 for informationsecurity,” Int. J. Sci. Res. in Computer Science and Engineering, vol. 8,no. 1, 2020.
8. M. Abu-Faraj, A. Al-Hyari, K. Aldebei, Z. Alqadi, and B. Al-Ahmad,“Rotation left digits to enhance the security level of message blockscryptography,” IEEE Access, pp. 69 388–69 397, 2022
9. Akeel, Wid & Alasady, Ali & Khalaf, Alaa. (2022). Hybrid information security system via combination of compression, cryptography, and image steganography. International Journal of Electrical and Computer Engineering. 12. 6574-6584. 10.11591/ijece.v12i6.pp6574-6584
10. Mustafa Sabah Taha et al 2019 IOP Conf. Ser.: Mater. Sci. Eng. 518 052003 DOI 10.1088/1757-899X/518/5/052003
11. Alotaibi, Muneera & Al-hendi, Daniah & Al Roithy, Budoor & Al Ghamdi, Manal & Gutub, Adnan. (2019). Secure Mobile Computing Authentication Utilizing Hash, Cryptography and Steganography Combination. Journal of Information Security and Cybercrimes Research. 2. 10.26735/16587790.2019.001.
12. Al-Juaid, N.A., Gutub, A.A. and Khan, E.A., 2018. Enhancing PC data security via combining RSA cryptography and video based steganography. Journal of Information Security and Cybercrimes Research, 1(1), pp.5-13.
13. Ria Das and Punyasha Chatterjee. 2017. Securing Data Transfer in IoT Employing an Integrated Approach of Cryptography & Steganography. In Proceedings of the International Conference on High Performance Compilation, Computing and Communications (HP3C-2017). Association for Computing Machinery, New York, NY, USA, 17–22. https://doi.org/10.1145/3069593.3069605
14. Al-Qwider, W.H. and Salameh, J.N.B., 2017. Novel technique for securing data communication systems by using cryptography and steganography. Jordanian Journal of Computers and Information Technology (JJCIT), 3(2), pp.110-130.

15. Jassim, K.N., Nsaif, A.K., Nseaf, A.K., Priambodo, B., Naf'an, E., Masril, M., Handriani, I. and Putra, Z.P., 2019, December. Hybrid cryptography and steganography method to embed encrypted text message within image. In Journal of Physics: Conference Series (Vol. 1339, No. 1, p. 012061). IOP Publishing.

16. Jasleen Kour,Deepankar Verma, Steganography Techniques –A Review Paper, International Journal of Emerging Research in Management &Technology

17. Ritu Sindhu, Pragati Singh, Information Hiding using Steganography, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958 (Online)

18. Hemalatha S , U. Dinesh Acharya , Renuka A, Wavelet transform based steganography technique to hide audio signals in image, e CC BY-NC-ND license.

19. Islam, S., Modi, M.R. & Gupta, P. Edge-based image steganography. EURASIP J. on Info. Security 2014, 8 (2014). https://doi.org/10.1186/1687-417X-2014-8 Published: 27 April 2014
DOI: https://doi.org/10.1186/1687-417X-2014-8

20. RigDas,Themrichon Tuithung, A Novel Steganography Method for Image Based on Huffman Encoding

21. Ramadhan Mstafa , Christian Bach, Information Hiding in Images Using Steganography Techniques, Norwich University March 14-16, 2013

22. Nagham Hamid,Osamah M. Al-Qershi,R. Badlishah Ahmad,Abid Yahya, Image Steganography Techniques: An Overview

23. Ashfaque Ahmed Memon,Mirza Adnan Baig,Riaz Ahmed Shaikh,Mirza Abdur Razzaq, Digital Image Security: Fusion of Encryption, Steganography and Watermarking

24. QI WU, MINHUI XUE, CONGBO MA, HU WANG, WENDY LA, OLIVIA BYRNES, Data Hiding with Deep Learning: A Survey Unifying Digital Watermarking and Steganography

25. Thomas Mittelholzer, An Information-Theoretic Approach to Steganography and Watermarking

26. Ronak Doshi, Pratik Jain, Lalit Gupta, Steganography and Its Applications in Security

27. Ross J. Anderson and Fabien A. P. Petitcolas, On the Limits of Steganography

28. Haripriya Rout , Brojo Kishore Mishra, Pros and Cons of Cryptography, Steganography and Perturbation techniques, IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834,p- ISSN: 2278-8735.

29. Pranali R. Ekatpure, Rutuja N Benkar, A Comparative Study of Steganography & Cryptography, International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064

30. Mustafa Sabah Taha et al 2019 IOP Conf. Ser.: Mater. Sci. Eng. 518 052003

31. IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 9, Issue 1, Ver. IV (Jan. 2014), PP 69-73 www.iosrjournals.org www.iosrjournals.org 69 | Page Digital Image Encryption Based on RSA Algorithm Ali E. Taki El_Deen, El-Sayed A. El-Badawy, Sameh N. Gobran

32. Image Cryptography Using RSA Algorithm in Network Security S.Anandakumar, IJCSET(www.ijcset.net) | September 2015 | Vol 5, Issue 9,326-330

33. El-Khamy, S.E., Korany, N.O. & El-Sherif, M.H. A security enhanced robust audio steganography algorithm for image hiding using sample comparison in discrete wavelet transform domain and RSA encryption. Multimed Tools Appl 76, 24091–24106 (2017). https://doi.org/10.1007/s11042-016-4113-8