Study of Data Hiding Techniques by Using Hashing Algorithm

Sarjil A Samad satware Farah A Samad Gothekar Muskan Nasir Bebal Swaliha Mansoor Khanzada

Department of IT GMVSC Tala University of Mumbai
Department of IT GMVSC Tala University of Mumbai
Department of IT GMVSC Tala University of Mumbai
Department of IT GMVSC Tala University of Mumbai

Prof.Raghvendra Singh

Assistant professor GMVSC & GMVIT
University of Mumbai

***Abstract*: - Advanced Image Steganography is used to develop a secure path for transferring or entering secret textbook dispatches. Using Chaff and Winnow & AES (Advanced Encryption Standard) encryption fashion, the textbook communication is translated and transferred to receiver veritably securely. The system uses AES encryption to cipher the stoner's secret textbook communication and crucial information while transferring it to receiver also using Diffie- Hellman crucial generation for participating secret key between sender and receiver.**

Keywords:-Advanced images steganography; chaff and winnow; AES, Diffie-Hellman; Encryption;

I. INTRODUCTION:

Steganography is the art of hiding and transmitting data through apparently innocuous carriers in an effort to conceal the existence of the data, the word Steganography literally means covered or hiding writing as derived from Greek. Steganography has its place in security. It is not intended to replace cryptography but supplement it. [1] Hiding a message with Steganography methods reduces the chance of a message being detected. If the message is also encrypted then it provides another layer of protection. The growing use of Internet needs to take attention while we send and receive personal information in a secured manner. For this, there are many approaches that can transfer the data into different forms so that their resultant data can be understood if it can be returned back into its original form. This technique is known as encryption. However, a major disadvantage of this method is that the existence of data is not hidden. If someone gives enough time then the unreadable encrypted data may be converted into its original form. A solution to this problem has already been achieved by using a "steganography" technique to hide data in a cover media so that other cannot notice it. The characteristics of the cover media depends on the amount of data that can be hidden, the perceptibility of the message and its robustness. In this document, I propose a new system for hiding data stands on many methods and algorithms for image hiding where I store on data file, called sink file in an image file called as container image. The primary objective is to use steganography techniques so as to provide more security and simultaneously using less storage. 7 Hidden information in the cover data is known as the "embedded" data and information hiding is a general term encompassing many sub disciplines, is a term around a wide range of problems beyond that of embedding message in content. The term hiding here can refer to either making the information undetectable or keeping the existence of the information secret. [1] Information hiding is a technique of hiding secret using redundant cover data such as images, audios, movies, documents, etc. This technique has recently become important in a number of application areas. For example, digital video, audio, and images are increasingly embedded with imperceptible marks, which may contain hidden signatures or watermarks that help to prevent unauthorized copy. It is a performance that inserts secret messages into a cover file, so that the existence of the messages is not apparent. [1] Research in information hiding has tremendous increased during the past decade with commercial interests driving the field. Although the art of concealment "hidden information" as old as the history, but the emergence of computer and the evolution of sciences and techniques breathe life again in this art with the use of new ideas, techniques, drawing on the computer characteristics in the way representation of the data, well known computer representation of all data including (Multimedia) is binary these representations are often the digital levels and areas and change values-aware of slight not aware or felt by Means sensual of human such as hearing, sight, the advantage use of these properties to hide data in multimedia by replace the values of these sites to the values of data to be hidden. Steganography is distinct from cryptography, but using both together can help improve the security of the protected information and prevent detection of the secret communication. If steganographically-hidden data is also encrypted, the data may still be safe from detection -- though the channel will no longer be safe from detection. There are advantages to using steganography combined with encryption over encryption-only communication. The primary advantage of using steganography to hide data over encryption is that it helps obscure the fact that there is sensitive data hidden in the file or other content carrying the hidden text. Whereas an encrypted file, message or network packet payload is clearly marked and identifiable as such, using steganographic techniques helps to obscure the presence of the secure channel.

II. LITERATURE REVIEW:

In the year of 2013 Soni, A.; Jain, J.; Roshan, R., The Fractional Fourier transform (FrFT), Investigated on as a generalization of the classical Fourier transform, introduced years ago in mathematics literature. The enhanced computation of fractional Fourier transform, the discrete version of FrFT came into existence DFrFT. This study of illustrates the advantage of discrete fractional Fourier transform (DFrFT) as compared to other transforms for steganography in image processing. The result shows same PSNR

in both domain (time and frequency) but DFrFT gives an advantage of additional stego key. The order parameter of this transform. In the year of 2013 Akhtar, N.; Johri, P.; Khan, S., implemented a variation of plain LSB (Least Significant Bit) algorithm.

The stego-image quality has been improved by using bit-inversion technique. LSB method improving the PSNR of stego image. Through storing the bit patterns for which LSBs are inverted, image may be obtained correctly. For the improving the robustness of steganography, RC4 algorithm had been implemented to achieve the randomization in hiding message image bits into cover image pixels instead of storing them sequentially. This method randomly disperses the bits of the message in the cover image and thus, harder for unauthorized people to extract the original message. The presented method shows good enhancement to Least Significant Bit technique in consideration to security as well as image quality. In the year of 2013 Prabakaran, G.; Bhavani, R. and Rajeswari P.S. Investigated on Medical records are extremely sensitive patient information a multi secure and robustness of medical image based steganography scheme is proposed.

This methodology provides an efficient and storage security mechanism for the protection of digital medical images. Authors proposed a viable steganography method using Integer Wavelet Transform to protect the MRI medical image into a single container image. The patient's medical diagnosis image has been taken as secret image and Arnold transform was applied and scrambled secret image was obtained. In this case, the scrambled secret image was embedded into the dummy container image and Inverse IWT was taken to get a dummy secret image.

It has been observed that the quality parameters are improved with acceptable PSNR compared to the existing algorithms. In the year of 2012 Thenmozhi, S. and Chandrasekaran, M., presented the novel scheme embeds data in integer wavelet transform coefficients by using a cropping function in an 8×8 block on the cover image. The optimal pixel change process has been applied after embedding the message. Authors employed the frequency domain to increase the robustness of our steganography method. Integer wavelet transform avoid the floating point precision problems of the wavelet filter.

Result shows that the method outperforms adaptive steganography technique based on integer wavelet transform in terms of peak signal to noise ratio and capacity. In the year of 2012 Das, R. and Tuithung, T. Proposed a novel technique for image steganography based on Huffman Encoding. Two 8 bit gray level image of size M X N and P X Q are used as cover image and secret image respectively. Huffman Encoding is performed over the secret image/message before embedding and each bit of Huffman code of secret image/message is embedded inside the cover image by altering the least significant bit (LSB) of each of the pixel's intensities of cover image. The size of Huffman encoded bit stream and Huffman Table are also embedded inside the cover image, in order that the StegoImage becomes standalone information to the receiver. Results show that the algorithm has a high capacity and a good invisibility. Moreover Peak Signal to Noise Ratio (PSNR) of stego image with cover image shows better result in comparison with other existing steganography approaches.

The satisfactory security is maintained in this research. In the year of 2012 Hemalatha, S, Acharya, U.D. and Renuka presented integer Wavelet Transform (IWT) is used to hide the key thus it is very secure and robust because no one can realize the hidden information and it cannot be lost due to noise or any signal processing operations. Result shows very good Peak Signal to Noise Ratio, which is a measure of security. In this method the secret information is hidden in the middle bit-planes of the integer wavelet coefficients in high frequency sub-bands. In the 2012 Reddy, H.S.M., Sathisha, N. and Kumari, A. Worked on the steganography is used to hide. Secure Steganography using Hybrid Domain Technique (SSHDT). The cover image of different formats and sizes are considered and resized to dimensions of power of 2. The Daubechies Lifting Wavelet Transforms (LWT) is applied on cover image to generate four sub bands XA, XH, XV and XD. The XD band is considered and divided into two equal blocks say upper and lower for payload embedding. The payload of different formats are considered and resized to dimensions of power of 2. The payload is fragmented into four equal blocks.

The Decision Factor Based Manipulation (DFBM) is used to scramble further stego object to improve security to the payload. Dubechies Inverse LWT (ILWT) is applied on XA, XH, XV and XD stego objects to obtain stego image in spatial domain. It has been observed that PSNR and embedding capacity of the proposed algorithm is better compared to the existing algorithm. With the rapid development of internet and wide application of multimedia technology, people can communicate the digital multimedia information such as digital image, with others conveniently over the internet. In numerous cases, image data, transmitted over a network are expected not to be browsed or processed by illegal receivers. Consequently, the security of digital image has attracted much attention recently and many different methods for image encryption have been proposed, such as Optical systems are of growing interest for image encryption because of their distinct advantages of processing 2-dimensional complex data in parallel at high speed.

In the past, many optical methods have been proposed in. Among them the most widely used and highly successful optical encryption scheme is double random phase encoding proposed in. It can be shown that if these random phases are statistically independent white noise then the encrypted image is also a stationary white noise. In some schemes, chaos based functions are used to generate random phase mask. Such as the generalization of the conventional Fourier transform.

The significance of network security is increased day by day as the size of data being transferred across the Internet. This issue pushes the researchers to do many studies to increase the ability to solve security issues. A solution for this issue is using the advantage of cryptography and steganography combined in one system. Many studies propose methods to combine cryptography

with steganography systems in one system. These methods were deceased in previous surveys available on the topic. This survey was published in 2014, it aims to give an overview of the method proposed to combine cryptography with steganography systems.

In this survey, the authors introduced 12 methods which are combined steganography and cryptography and made a comparative analysis. This comparative has been implemented on the basis of the requirements of security i.e. authentication, confidentiality, and robustness. Another survey was published in 2014, this survey presented many steganographic techniques combined with cryptography, AES Algorithm, Alteration Component, Random Key Generation, Distortion Process, Key Based Security Algorithm.

There has been a continuous rise in the number of data security threats in the recent past and it has become a matter of concern for the security experts. Cryptography and steganography are the best techniques to nullify this threat. The researchers today are proposing a blended approach of both techniques because a higher level of security is achieved when both techniques are used together.

III. PROBLEM DEFINITION:

In this project, we propose to develop a system to hiding data by using "STEGANOGRAPHY" technique as I used many methods stands on some techniques to have at the back-end a software for hiding data based on hiding algorithms.

After studying the data hiding algorithms we found many ways to hiding data by using the multimedia files and the main question for me was "Where hidden data hides?" as we found by our search to know where the data hides it's important to know what is the file type of the data that it shall be hidden and the cover file type so it is possible to alter image.

By the final of our research we developed a software uses an algorithm, to embed data in an image; The purposed system is called "Steganography", the aim of this project is to encrypt the data; the meaning of encrypt is to hide the data over an image using different steganographic algorithms, in this system cryptographic is the algorithms that we use to hiding the data.

Cryptography can be broken down into three different types:

- Secret Key Cryptography.
- Public Key Cryptography.
- Hash Functions.

Secret Key Cryptography:

In this cryptography method (also known as symmetric-key cryptography), the single key needed to encrypt and decrypt messages is a shared secret between the communicating parties. The biggest problem with this method is that the secret key must be communicated through an external mechanism separate from the communication channel over which the encrypted text flows. In addition, secret-key systems do not support digital signatures. These limitations are addressed in public-key cryptography (see separate entry).Symmetric cryptography a secret key (or “private key”) is a piece of information or a framework that is used to decrypt and encrypt messages.in Each party to a conversation that is intended to be private possesses a common secret key. Using the key one party sends the other a message transformed from its original (plaintext) into its encrypted form (ciphertext) and the other party reverses this process to reveal the original, and the process repeats. Examples of a secret key are ROT13 as agreed upon by the parties or a cable television provider’s sending of Entitlement Management Messages (EMMs) alongside programming. In the latter, the viewer’s set-top box contains the secret key that the cable provider and viewer use to make the programming viewable. A common challenge in symmetric or secret key encryption systems is agreeing upon the private key when the parties are unable to meet in person, since someone may eavesdrop on the key sharing discussion. For that reason, asymmetric or public-key cryptography can be used to share a key. In asymmetric cryptography or encryption, the parties use a private key and a public key (hence public-key cryptography [PKC] being synonymous with the asymmetric variety).

Public Key Cryptography:

Public-key cryptography, or asymmetric cryptography, is the field of cryptographic systems that use pairs of related keys. Each key pair consists of a public key and a corresponding private key. Key pairs are generated with cryptographic algorithms based on mathematical problems termed one-way functions. Security of public-key cryptography depends on keeping the private key secret; the public key can be openly distributed without compromising security.

In a public-key encryption system, anyone with a public key can encrypt a message, yielding a ciphertext, but only those who know the corresponding private key can decrypt the ciphertext to obtain the original message.

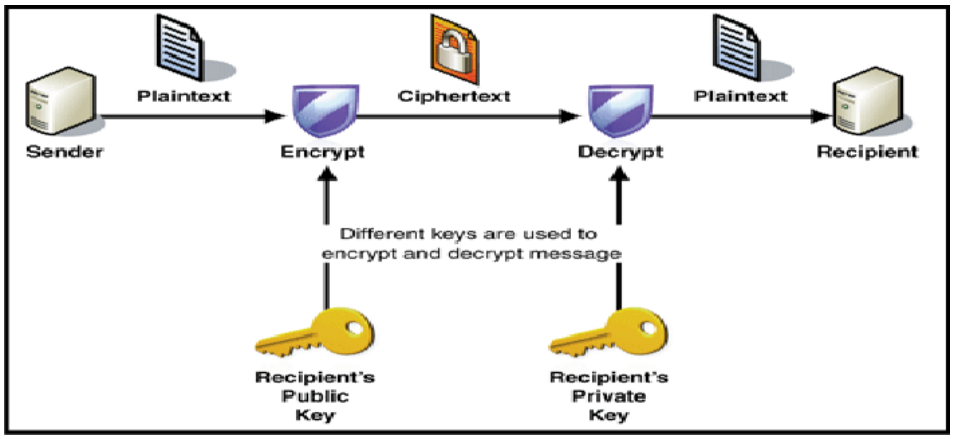

Fig 1

For example, a journalist can publish the public key of an encryption key pair on a web site so that sources can send secret messages to the news organization in ciphertext. Only the journalist who knows the corresponding private key can decrypt the ciphertexts to obtain the sources' messages—an eavesdropper reading email on its way to the journalist can't decrypt the ciphertexts. However, public-key encryption doesn't conceal metadata like what computer a source used to send a message, when they sent it, or how long it is. Public-key encryption on its own also doesn't tell the recipient anything about who sent a message—it just conceals the content of a message in a ciphertext that can only be decrypted with the private key.

Hash Functions:

A cryptographic hash function is an algorithm that takes an arbitrary amount of data input—a credential—and produces a fixed-size output of enciphered text called a hash value, or just "hash."
That enciphered text can then be stored instead of the password itself, and later used to verify the user.

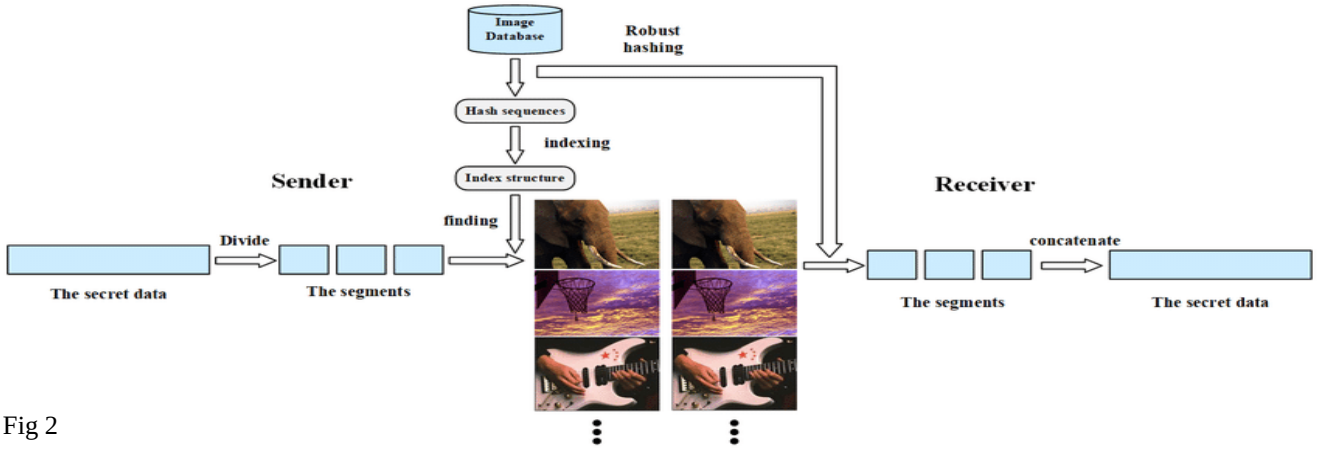

Fig 2

Features of Hash Functions:

The typical features of hash functions are −

- **Fixed Length Output (Hash Value):**
  - Hash function coverts data of arbitrary length to a fixed length. This process is often referred to as **hashing the data**.
  - In general, the hash is much smaller than the input data, hence hash functions are sometimes called **compression functions**.
  - Since a hash is a smaller representation of a larger data, it is also referred to as a **digest**.
  - Hash function with n bit output is referred to as an **n-bit hash function**. Popular hash functions generate values between 160 and 512 bits.
- **Efficiency of Operation:**
  - Generally for any hash function h with input x, computation of h(x) is a fast operation.
  - Computationally hash functions are much faster than a symmetric encryption.

IV. PROBLEM SOLUTION:

This project addresses the security problem of transmitting the data over internet network, the main idea coming when we start asking that how can us send a message secretly to the destination? The science of steganography answers this question. Using steganography, information can be hidden in image. In this document, we proposed some methods and algorithms of an image steganography system to hide a digital text of a secret message.

V. PROCESS METHODOLOGY AND APPROACH:

We use python language for our project Image Steganography.

A data flow diagram (DFD) is a graphical representation of the "flow" of data through an information system, modelling its process aspects. Often they are a preliminary step used to create an overview of the system which can later be elaborated. DFDs can also be used for the visualization of data processing (structured design). A DFD shows what kinds of information will be input to and output from the system, where the data will come from and go to, and where the data will be stored. It does not show information about the timing of processes, or information about whether processes will operate in sequence or in parallel.

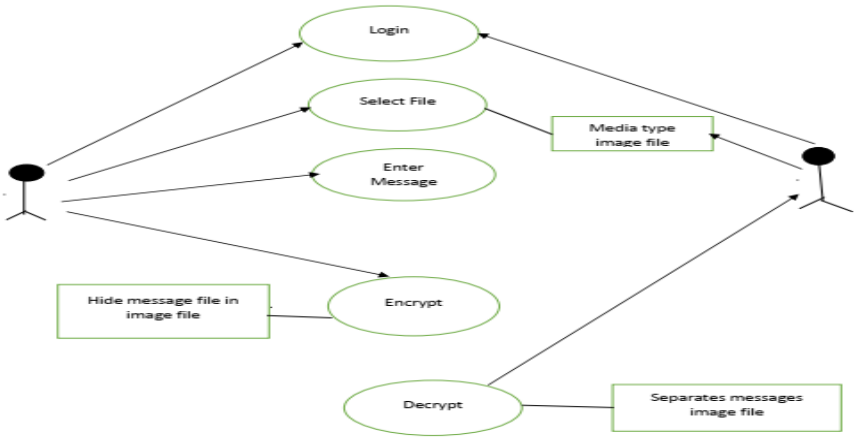

Fig 3

CONCLUSION: Hence we had studied about Image Steganography and we will implement in further process.

REFERENCES:

[1]. Soni, A.; Jain, J.; Roshan, R., "Image steganography using discrete fractional Fourier transform," Intelligent Systems and Signal Processing (ISSP), 2013 International Conference on , vol., no., pp.97,100, 1-2 March 2013.

[2]. Akhtar, N.; Johri, P.; Khan, S., "Enhancing the Security and Quality of LSB Based Image Steganography," Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on, vol., no., pp.385, 390, 27-29 Sept. 2013.

[3]. Das, R.; Tuithung, T., "A novel steganography method for image based on Huffman Encoding," Emerging Trends and Applications in Computer Science (NCETACS), 2012 3rd National Conference on , vol., no., pp.14,18, 30-31 March 2012.

[4]. Hemalatha, S.; Acharya, U.D.; Renuka, A.; Kamath, P.R., "A secure image steganography technique using Integer Wavelet Transform," Information and Communication Technologies (WICT), 2012 World Congress on , vol., no., pp.755,758, Oct. 30 2012-Nov. 2 2012.

[5]. Prabakaran, G.; Bhavani, R.; Rajeswari, P.S., "Multi secure and robustness for medical image based steganography scheme," Circuits, Power and Computing Technologies (ICCPCT), 2013 International Conference on , vol., no., pp.1188,1193, 20-21 March 2013.

[6]. Thenmozhi, S.; Chandrasekaran, M., "Novel approach for image stenography based on integer wavelet transform," Computational Intelligence & Computing Research (ICCIC), 2012 IEEE International Conference on, vol., no., pp.1, 5, 18-20 Dec. 2012.

[7]. Reddy, H.S.M.; Sathisha, N.; Kumari, A.; Raja, K.B., "Secure steganography using hybrid domain technique," Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference on , vol., no., pp.1,11, 26-28 July 2012.

[8]. Masud Karim, S.M.; Rahman, M.S.; Hossain, M.I., "A new approach for LSB based image steganography using secret key," Computer and Information Technology (ICCIT), 2011 14th International Conference on, vol., no., pp.286, 291, 22-24 Dec. 2011.

[9] Lin Zhang, Jianhua Wu, Nanrun Zhou, "Image Encryption with Discrete Fractional Cosine Transform and Chaos", Fifth International Conference on Information Assurance and Security 2009 IAS '09, pp 61 – 64, 2009.

[10] Ran Tao, Yi Xin, Yue Wang, "Double image encryption based on random phase encoding in the fractional Fourier domain", Optics Express, Vol. 15 Issue 24, pp 16067- 16079, 2007.