RESEARCH ARTICLE OPEN ACCESS

THE ART OF SECRET COMMUNICATION AND PROTECTION

Devika Rani Roy, Kris D'Souza, Aaradhya Desai, Dhananjay Khedkar

Department of Information Technology

K.C. College of Engineering and Management Studies and Research

Thane, India

--*********************---

Abstract: Nowadays security is a big concern when it comes to cyber space. There are multiple applications that provide security to an infrastructure and to a network yet they still somehow have loopholes through which hackers exploit the system. This happens on a large scale and also on small scale infrastructures.

Our project tries to add an extra layer of security that all kinds of infrastructures and networks can implement. It works by helping encrypt the data before being shared and hence adding a new layer to the already existing security systems. This system when combined with the already existing HTTPS protocol can help project confidentiality and authenticity and tries to minimize the risk of information leakage in an already compromised network. At the same time this system is easy to implement and is cost effective. It is very easy to learn so new employees and even employees with non-IT backgrounds can learn it within a few minutes. It is accessable and very user friendly.

Data hiding is the art of hiding data for various purposes such as; to maintain private data, secure confidential data and so on. Securely exchanging the data over the internet network is a very important issue. So, in order to transfer the data securely to the destination, there are many approaches like cryptography and steganography. In this project we propose a LSB & DCT-based steganographic method for hiding the data by applying Least Significant Bit (LSB) algorithm for embedding the data into the images which is implemented through the Microsoft .NET framework using the C#.NET.

Securing data encryption and decryption using Cryptography and Steganography techniques. Due to recent developments in stego analysis, providing security to personal contents, messages, or digital images using steganography has become difficult. By using stego analysis, one can easily reveal the existence of hidden information in carrier files. This project introduces a novel steganographic approach for communication between two private parties. The approach introduced in this project makes use of both steganographic as well as cryptographic techniques. In Cryptography we are using RSA. In Steganography we are using Image Steganography for hiding the data. And we also use the Mutual Authentication process to satisfy all services in Cryptography i.e., Access Control, Confidentiality, Integrity, Authentication. In this way we can maintain the data more securely. Since we use the RSA algorithm for securing the data and again on this we perform Steganography to hide the data in an image. Such that any other person in the network cannot access the data present in the network. Only the sender and receiver can retrieve the message from the data.

Keywords: *Steganography, Encryption, Decryption, Password Strength, Breach detection.*

--*********************---

1. INTRODUCTION

Nowadays people use the internet without any caution and that habit has lead to people using the same habit in the corporate world. The problem with this is corporate systems are more likely to be attacked rather than a personal system. This is the reason why there has to be a client side protection initiative to protect corporate confidentials being shared on the corporate systems.

Hackers these days are a step ahead of the cyber defences used in corporations. Also it is not possible to have a very advanced cyber defence system by every corporation .

Hence our project comes in to provide a security solution to corporates of all levels and adding a layer of defence to the corporate network.Our project is easy to use.Our project is easy to be learnt by new employees and Non-IT background based employees.

Our project helps to minimize the risk of confidentiality breach in already compromised systems.It uses modern and energy efficient encryption algorithms to provide safer ways of sharing documents, images and texts.

It requires less computational power as well and is also very quick.

It will work on almost all modern day systems and even some of the legacy systems.

Also now systems and features can be easily added to it.

The growing use of the Internet needs to take attention while we send and receive personal information in a secure 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 others 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 a data file, called a sink file in an image file called a container image. The primary objective is to use steganography techniques so as to provide more security and simultaneously use less storage.

2. LITERATURE SURVEY

There has been a large amount of development in information technology in recent times. Hence it has become crucial that we protect the sensitive information by implementing encryption in our daily life. AES is one of the best existing symmetric key algorithms to provide encryption. AES can be implemented on both hardware as well as on software. AES is a non-Feistel cipher. AES can encrypt and decrypt a data block of 128 bits. It does this by using 10, 12, or 14 rounds and the key size can be 128, 192, or 256 bits respectively depending upon the roungs being used. In this paper, the software Xilinx ISE project navigator is being used for simulation for encryption.[1]

The Advanced Encryption Standard (AES) algorithm is one of the most common and widely used symmetric key cipher algorithms in the world. This algorithm has its very own particular structure that encrypts and decrypts data and can be applied in hardware as well as software. It is nearly impossible for hackers to get the real data when encrypted using the AES algorithm. Till now there are zero evidence that proves the cracking of this algorithm.[2]

One of the primary goals of cryptography is to ensure confidentiality and integrity. There are other goals of communication security, such as guaranteeing authenticity of communications and availability and non- repudiation. Cryptography is used widely and if a person uses online transactions using credit cards, debit cards etc. Cryptography must be used to ensure security. This helps to ensure the privacy of any type of card use. In electronic banking, cryptography is used to ensure that checks can be unforgeable.[3]

The NIST has standardized the SHA-2 family as part of the Secure Hash Standard in the FIPs 180-4. This standard is not superseded by the upcoming SHA-3 standard. Rather, the SHA-2 family is supplemented by the SHA-3. Thus, it is likely that the SHA-2 family will remain as ubiquitously deployed in the foreseeable future as it is now. Therefore, the continuous application of the Hashing algorithms of the SHA family is crucial and will continue in the modern world.[4]

It is a simple method that provides good values for MSE and PSNR. Messages can be easily hacked by an attacker having programming experience therefore, LSB method is not secure enough. To improve the security of LSB and to protect the secret information from being hacked and exposed to the hacker or an attacker, an additional stage is added. This particular stage adds an important protection keeping the same quality parameters and the efficiency of LSB.[5]

In recent times, the demand for the Internet is increasing daily, when it comes to data transmission or other types of multimedia on the Internet. It is the service providers responsibility to ensure the necessary protection against data-theft attacks and to provide services in a timely manner. This article compares the frequently used data encryption algorithms. The main focus of this paper is to find out and assess the performance of different algorithms when using various data loads in different settings**.**[6]

This article contains covert communication methods using encryption. A method used to protect sensitive data. Secret messages are encrypted with block ciphers based on the two encryption algorithms which are Data Encryption Standard (DES) and Triple Data Encryption Algorithm (TDEA), which were used by federal agencies to protect sensitive data. This algorithm perfectly defines the mathematical steps considered essential to convert data into a cryptographic cipher text and convert the cipher text back into its original form with a block length of 128 bits and with a key size of 256 bits. This article compares the performance and power usage of the most common encryption algorithms which are DES, 3DES, AES, and Blowfish.[7]

The main goal of this article is to improve the overall reliability of the AES algorithm to provide a more secure communication network over the Internet. The Rijndael algorithm was chosen as the advanced encryption standard. The AES algorithm gives much more security without limitations. Recently, however, cryptanalysts have discovered several ways to break AES. To solve this, we need to increase the number of rounds in the AES algorithm.[8]

A methodology for analyzing the energy efficiency and performance of hashing algorithms on mobile devices and measuring energy on Java-enabled smartphones is described. Evaluate the energy efficiency of 17 hash functions namely Adler32, Crc16, Crc32, Haval256, MD2, MD4, MD5, MD6, SHA1, SHA224, SHA256, SHA384, SHA512, Skein, SV1, Tiger and Whirlpool with the help of battery-based GSM do. Modem method charge measurements and quality are judged or assessed by using Avalanche and Chi-square tests. The results that we get shows us the most energy efficient hash functions on mobile devices are SV1 for cryptographic applications and crc16 for non-cryptographic applications.[9]

The primary aim of this paper is to evaluate an image encryption algorithm developed based on wavelet decomposition of images. The encryption algorithms Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are used only to encrypt wavelet decomposition granularity coefficients, and the encrypted image is the resultant of inversed wavelet transform. During the encryption process compressed data is also verified. This encryption scheme is implemented in the Matlab environment.[10]

3. SCOPE

The scope of the project is implementation of steganography tools for hiding information including any type of information file and image files and the path where the user wants to save image and extruded file. We will use LSB technique; the proposed approach is to use the suitable algorithm for embedding the data in image files; we will show a brief of this algorithm that we used to hide data.

This work presents a scheme that can transmit large quantities of secret information and provides secure communication between two private parties. Both steganography and cryptography can be woven in this scheme to make the detection more complicated. Any kind of text data can be employed as secret msg. The secret message employing the concept of steganography is sent over the network. In addition, the proposed procedure is simple and easy to implement.

4. FEASIBILITY STUDY

Technical Feasibility:

Analysis of technical resources available in the organizations concerning the project requirement comes under technical feasibility.

This code is developed in VScode and will be implemented as a Web based application with cybersecurity at the core. Hence it is completely feasible.

Operational Feasibility:

This project adds a new layer of security to the already existing system.

This is done keeping all the already existing settings and system as it is and still adding security with ease of use.

Economic Feasibility:

Our application will be a web based application hence it will be very economical.

Additionally we have used encryption algorithms which are energy efficient and can work the best in the given environment.

5. METHODOLOGY

File Encryption Tool:

For file encryption we use SHA-256 and AES-256 hashing and encrypting algorithms. SHA is a Hashing algorithm which gives a hash size of 256 bytes. AES is an encryption algorithm which has a key size of 36 bytes and output of 256 bits. Algorithms used here are more energy efficient as compared to their competing counterparts. The other competing algorithms like MD5, DES, 3DES, RSA, SHA-512 etc consume more power and have low efficiency and at the same time take more time to compute. Also the chosen algorithms work on legacy systems.

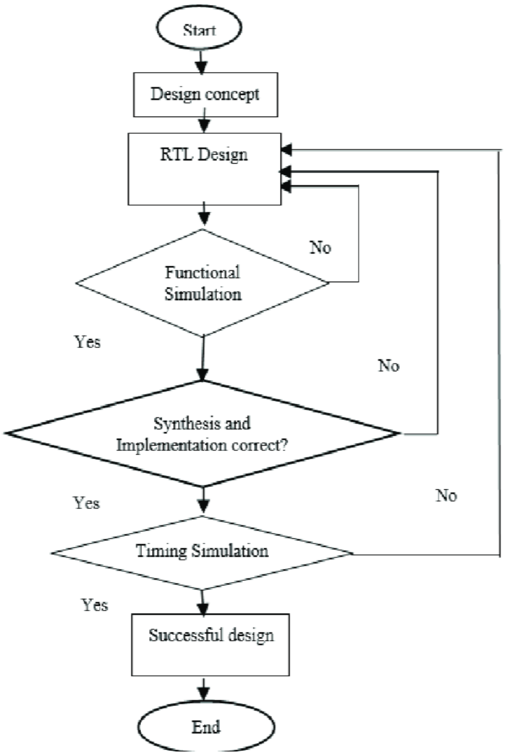


Fig. 1: SHA-256 Diagram

In File Encryption, the user is asked for a password and then that password is applied with the hash function and a hash is generated. That hash is then used as a key for AES. AES uses the hash as key and encrypted the file as a result the generated output of any type of file is a set of strings that are not readable by any user and to decrypt the file the same hash is used and the same password has to be provided. The resultant is the original file that you uploaded. This works on all types of files.

Text Encryption Tool:

In this section, we use AES-256 to encrypt the text that has to be encrypted. AES-256 was chosen for this as it is very secure, provides great security and is the most efficient algorithm when it comes to working on legacy systems and systems with low computing power. Other algorithms that were tested were DES, 3DES, RSA and many more. AES works with 3 types, with 128 bit key, 192 bit key and 256 bit key with 10,12 and 14 rounds respectively.

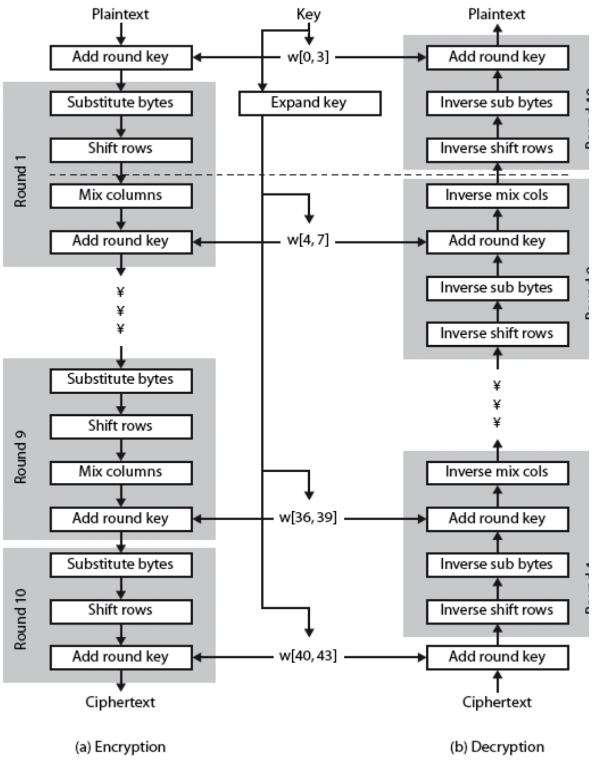


Fig. 2: AES Diagram

The way it works is that the user is asked for a password that will be used as the key that will encrypt the text. This text is later encrypted and then the output is given. Along with this output, an Initalization Vector(I.V) is formed. This can be sent to the receiver through different channels. At the time of decryption, this I.V and the password has to be put in the decryption parameters. The result is your text in its original form

Steganography Tool:

Modifying the cover picture's least significant bits (LSB) is the first step in using the LSB steganography technique to conceal an image. This can be accomplished by multiplying and dividing each pixel value by 16, which effectively sets the LSB of each pixel to zero.

The most significant bits (MSB) of the secret image are multiplied by 16 in order to ensure that the secret image has the same bit depth as the cover image. The cover picture can then be added to the resultant image, together with the associated pixel values, to create the stego image.

The LSB of each colour channel (red, green, and blue) must be extracted from the stego image by taking the modulo 16 of each pixel value and multiplying the outcome by 16. The hidden image can be produced by combining the extracted LSBs with another image.

Overall, the LSB steganography technique is a reliable and efficient way to conceal information in photographs without materially affecting the quality of the image or losing any important data.

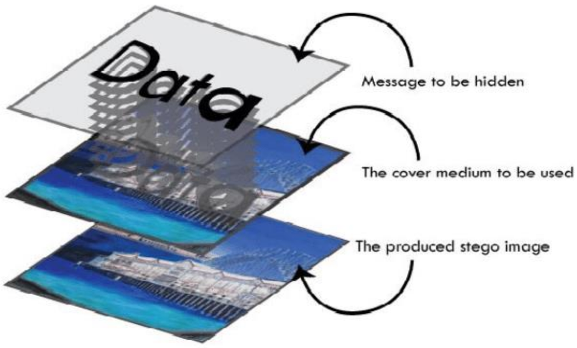


Fig. 3: Steganography

Password Tools:

This section contains three main sections. Password generation, password strength checker and password breach detection.

Password Generator Tool:

This will ask the user to enter the length of the password that they desire to generate. After entering the value, the output will be of that length and the password will be containing small case, large case, numeric and symbols in it making it a string password which will take a lot of time to breach. This generated password will be unique.

Password Strength Checker Tool:

We check if the password contains a small case, large case, numeric and symbols in it. The password you have or password generated can be entered here and the time required to crack the password will be displayed. This will also show various other precise data about the password you've entered.

Password Breach Detection Tool:

This part of the project works of "HAVE I BEEN PAWNED" api. This is an open source database which updates its data on regular bases and has up-to-date data about passwords that have been breached in data breaches. This will tell the user about how many data breaches had the same password that they entered.

Here the user is given a parameter or an input box where the user can put their desired password and they will receive the number of data breaches that had the same passwords that they entered.

6. FUNCTIONAL REQUIREMENTS

Hardware requirements:

- Any computer with motherboards after 2005.
- Processors having AES flags or at least processor with processing capacity equal to Intel IA-32 Pentium 3rd or 4th gen.
- Internet connection is mandatory.
- Virtual Memory is Optional.
- RAM required is at least 2GB.

Software requirements:

- WEB browser.
- VSCODE

7. PRODUCT DESIGN

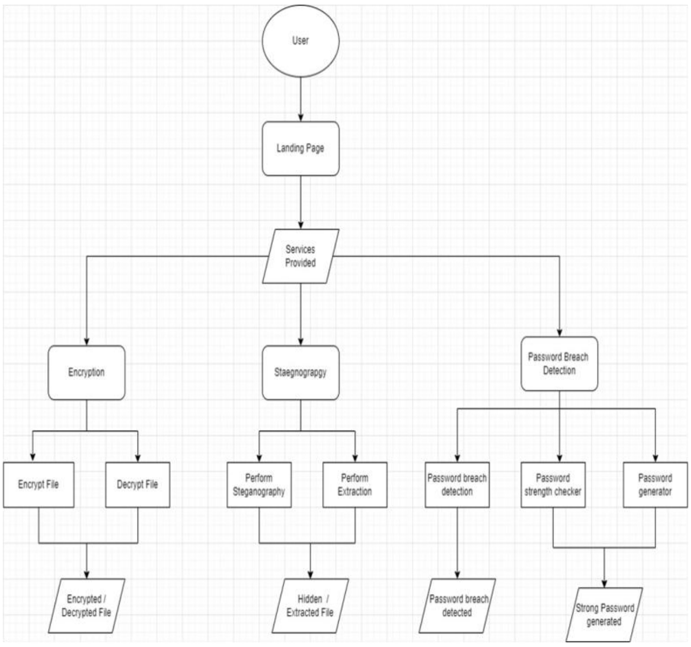
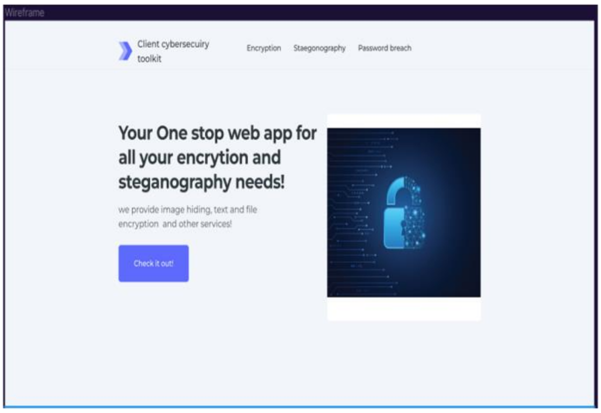


Fig. 4: Product Design Chart

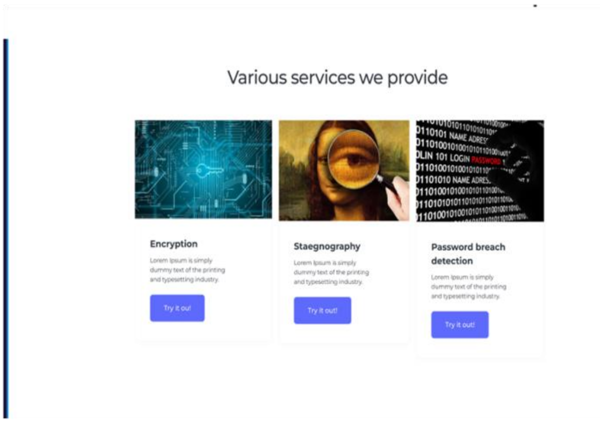
8. RESULT



Your One stop web app for all your encrytion and steganography needs!

we provide image hiding, text and file encryption and other services!

Fig. 5: Landing page



Various services we provide

Encryption

Lorem Ipsum is simply dummy text of the printing and typesetting industry.

Staegnography

Lorem Ipsum is simply dummy text of the printing and typesetting industry.

Password breach detection

Lorem Ipsum is simply dummy text of the printing and typesetting industry.

Fig. 6: Services page

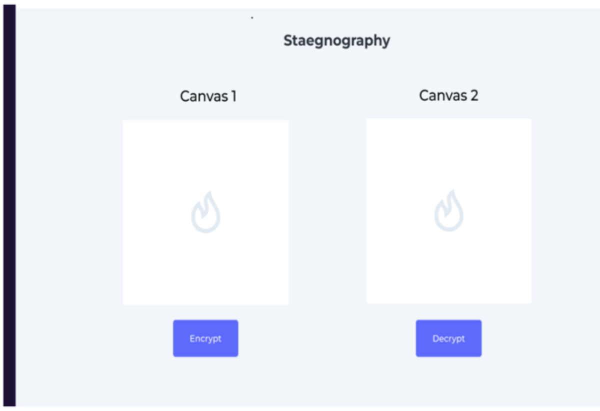


Fig. 7: Steganography page

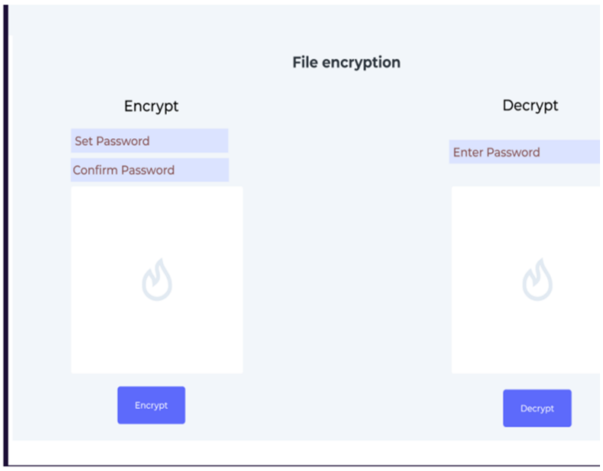


Fig. 8: File Encryption and Decryption page

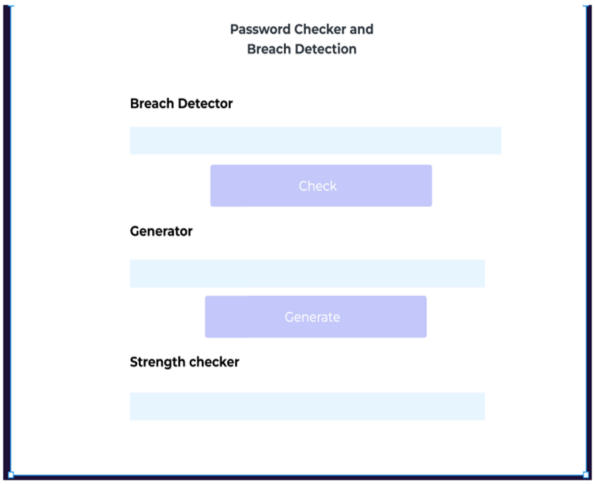


Fig. 9: Password breach detector, strength checker and generator

9. CONCLUSION

Hence made a system that helps corporates establish a new security level at the client level to share their corporate secrets and make communication in corporates much more safer. Also being a step ahead, my hiding the messages being transmitted from the hackers that are currently monitoring or intercepting the corporate network, in an energy efficient and being very affordable.

10. FUTURE SCOPE

This project can be used by organizations that do not have a budget for a full size cyber security. This project helps clients with providing security at the network level and also helps work on networks that are compromised. In the future, more efficient algorithms can be added to the system. At the same time new features can be added like phishing website detection can be added. This project can also be launched as a product.

ACKNOWLEDGEMENT

We record our heart-felt gratitude and indebtedness to our guide Prof. Devika Rani Roy. for supervising us care and zeal throughout our project “THE ART OF SECRET COMMUNICATION AND PROTECTION”.

We would like to thank Principal Dr.Vilas Nitnaware And Prof. Amarja Adgaonkar (HOD OF IT DEPT) of our prestigious institute for his helpful guidance and encouragement.

We are immensely thankful to all the respected teachers of the IT Department for the help that they offered to us with affectionate understanding whenever we needed it.

REFERENCES

[1] International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 03 Issue: 05 | May-2016 www.irjet.net p-ISSN: 2395-0072 An Efficient Symmetric Cipher Algorithm for Data Encryption

[2] A compact FPGA-based processor for the Secure Hash Algorithm SHA-256, Rommel García , Ignacio Algredo-Badillo, Miguel Morales-Sandoval, Claudia Feregrino-Uribe, René Cumplido 2013

[3] IJCSMC, Vol. 11, Issue. 1, January 2022, pg.182 – 193 Carrier Image Rearrangement to Enhance the Security Level of LSB Method of Data Steganography Prof. Mohamad K. Abu Zalata; Dr. Mohamad T. Barakat; Prof. Ziad A. AlqadiAlbalqa Applied University, Faculty of Engineering Technology, Jordan, Amman DOI: 10.47760/ijcsmc.2022.v11i01.024

[4] Volume: 04 Issue: 05 | May -2017 www.irjet.net p-ISSN: 2395-0072 © 2017, IRJET | Impact Factor value: 5.181 | ISO 9001:2008 Certified Journal | Page 2926 Image Steganography and Data hiding in QR Code Rutuja Kakade1, Nikita Kasar2, Shruti Kulkarni3, Shubham Kumbalpuri4, Sonali Patil5

[5] Analysis of SHA-512/224 and SHA-512/256 Christoph Dobraunig, Maria Eichlseder & Florian Mendel, First Online: 30 December 2015

[6] International Journal of Scientific Engineering and Research (IJSER) www.ijser.in ISSN (Online): 2347-3878 Volume 2 Issue 11, November 2014

[7] Image encryption algorithms based on wavelet decomposition and encryption of compressed data in wavelet domain, PRZEGLĄD ELEKTROTECHNICZNY, ISSN 0033-2097, R. 94 NR 2/2018

[8] The International Arab Journal of Information Technology, Vol. 16, No. 1, January 2019 A Steganography Scheme on JPEG Compressed Cover Image with High Embedding Capacity

[9] Journal of Theoretical and Applied Information Technology 15th January 2020. Vol.98. No 01 ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195 78 AN EFFECTIVE AND SECURE DIGITAL IMAGE STEGANOGRAPHY SCHEME USING TWO RANDOM FUNCTION AND CHAOTIC MAP 1 MOHANAD NAJM ABDULWAHED

[10] ISSN 22773061 1164 | PageJuly25,2013 Comparative Study of DES, 3DES, AES and RSA Amritpal Singh, Mohit Marwaha, Baljinder Singh, Sandeep Singh