**Image Based Encyption Technique**

**Overview**

**Literature Survey**

We can classify passwords as the most important and crucial resource being stored in the database. Hence, in the past extensive research has been done and a lot of researchers from around the world have published their research about its security, attacks on the database system, password attacks, innovative ways of performing those attacks and defense systems against them. Some recommended the use of images or separate use of steganography and cryptography for user authentication, while some suggested the combination of steganography and cryptography for the same. Considering the fact that each one of them had some strengths and weaknesses that sometimes they significantly shielded the system or failed due to some gaps in their method of implementation.

**2.1. Image authentication**

In [6] the authors proposed an image-based authentication system with the use of steganography. Highlighting the issues with current authentication systems such as, having to remember the alphanumeric passwords and people having a number of user accounts on the internet they accidentally or lazily set the same password for multiple user accounts which is a potential security threat. They suggest an innovative system where the password is hidden behind a secret image using steganography and stored in the database. At the time of sign up, a traditional process is followed but the user is also asked to browse and provide a secret image that has the password embedded in it. The user details with the password embedded secret image stored in the server database. Next time the user logs in, the login interface sends the username in plaintext and the secret image is sent in the bit stream. They argue that in case the password and the secret image is known to the attacker, it would still be impossible for them to penetrate through the system as the database not only compares the images and the passwords but also the dimensions of the image [6]. However, in [7] a unique way has been introduced for user authentication. In their exceptional way of authentication, they used a clickbased graphical password scheme which is a cued-recall graphical password technique. Basing their research on Passpoint [8], which was proposed in 2005, where the password was composed of numerous points anywhere on the image. They also suggested a "robust discretization" system with a variety of conflicting grids enabling login attempts to be recognized that strongly resembled with the correct form and translating the password inserted into a key for cryptographic authentication. Hence, CCP proposed an alternative way to it using the hotspot technique. Rather than clicking on multiple points on a single image, the user has to click on one point on each image as there would be multiple images to be clicked by the user. The authors conclude by arguing that the CCP is securer than the graphical authentication methods that have been introduced previously. Resulting in which, it makes it difficult for the attackers to acquire the correct sets of images for the user and then analyze the correct hotspots on each of those images [7].

**2.2. Steganography and cryptography**

In the past, a lot of researchers have directed their research towards the combination of two or more security measures. Therefore, steganography and cryptography have been the most relied one by them. Considering the fact, that steganography itself applies cryptography while hiding the text behind. Hence, [9] explain the way of using steganography and encryption to make the data secure. They suggest that Elliptic Curve Cryptography can be used for image encryption Huffman Coding method for image steganography, and Discrete Wavelet Transform for image compression. In their work, they argue that the Elliptic Curve Cryptosystem is the most secure one out of all the existing cryptosystems. Most importantly by comparing the Elliptic Curve Cryptosystem with Diffie-Hellman or RSA, they highlight that it provides the same level of security with much shorter keys. Provided that, it offers higher speeds, lesser power consumption, bandwidth savings, and storage efficiencies. This could particularly be useful where processing capacity, bandwidths, power availability or storage are required [9]. As well as in [10] the researchers are using the combination of security measures like steganography and cryptography to make the system secure. But with a different method as they proposed a blend of steganography with the use of discrete cosine transform (DCT) and cryptography using the one-time pad or vernam cipher implemented on a digital image and measuring the quality of the image using the peak signal to noise ratio (PSNR) and the quality of the extraction of the decrypted message using Normalized Cross Correlation (NCC). They proposed an embedding algorithm to perform this operation. The results were measured in Peak Signal to Noise Ratio (PSNR) and Mean square error (MSE). The smaller value of the MSE depicted the better quality of the output image. In the final result, the average value of the MSE was 0.50232 which proved to be a reliable way of implementing a combination of cryptography and steganography. Also, they suggested that encryption methods such as AES, RSA, and DES could be considered to be combined with steganography in future [10]. Few researchers tried to go one step ahead and use the renowned and stronger encryption algorithms as they are considered, such as AES and RSA. While few tried to modify the existing one or combine them with other algorithms like SHA512 and MD5. According to [11] integrating AES and RSA together and applying steganography elevates the security of the system. In their research, they propose a combined and alternative approach to secure the system using cryptography and steganography. They used two encryption algorithms, AES (with symmetric keys) and RSA (with asymmetric keys) with image steganography. To justify their choice, they mention that combining these three techniques together helps to construct a strong communication system based on steganography that can sustain several types of cyberattacks, reverse engineering and detection systems. The entire operation has three main components: sending, transmitting and receiving. The sender uses three inputs for the communication, secret data to be transmitted, cover image to hide the secret data and the public RSA key of the receiving party. By using the private RSA key, the steganographic image, receiver decrypts the secret data. Their system used AES-128 for primary encryption. With each new communication string, the encryption key (128 bits) is formed and consists of two parts: calculated and random, both being128-bit in size. a pseudo-random pattern generator (PRPG) seeded with either variable or constant data is used to generate the 1st half of the AES Key which is a random part of the key. Non-volatile color information (NVCI) is used to calculate the computed part of the encryption key which is the 2nd half of the AES Key. Using a powerful algorithm such as SHA512, MD5, the high order bits of each color channel (RGB in a color image) are hashed. Also, it needs to be noted that only half of the hash value is used in the 2nd half of the AES key. The data is embedded in the image using the data rearrangement method and LSB pixel mapping. The steganographic image travels through any communication channel like email, network, file sharing, etc. and in the end, the receiver’s system processes the VCI part of the steganographic image to decrypt it. The receiver’s system recovers the 1st and the 2nds half of the AES key. In the end, the receiver decrypts the intended secret data after retrieving both the halves of the AES key [11]. Research done in [12] also introduced the same combined approach to ensure the security of the data by merging steganography and cryptography using the AES-128 algorithm but they also modified the existing AES algorithm. They mentioned that security operations take place in parts to achieve two levels of security. In the two parts of their research, in the first part, they modified the AES algorithm to accommodate the steganography method that they implemented, and it is called AES\_MPK algorithm and in the second part, the same AES\_MPK algorithm is merged with the steganography algorithm to hide the encrypted secret behind the image. To perform the first part of the operations, the authors required the output in the form of MPK digits as MSLDIPMPK and PVD\_MPK methods use the MPK digits for hiding the data. Hence, the revised AES algorithm was called AES\_MPK algorithm. And in the second part, they encrypted the message M using AES\_MPK algorithm using the key K and produce the ciphertext. Later the same ciphertext is hidden behind the cover image C using the MSLDIP-MPK and PVD\_MPK methods to produce the steganographic image S. They conclude that with the implementation of their proposed method it would be easier to transmit the data even over the open channels as the ciphertext would not fetch the unwanted attention as it is hidden behind the image and it is capable of hiding a large amount of information than existing methods. Also, their system provides two layers of security making the system even more secure [12].

**2.3. Evaluation of cryptography algorithms**

While giving attention to the multi-layered and decentralized security measure, it is very crucial to choose the method that is more reliable and flexible. Some researchers have written papers where they have compared and evaluated the existing cryptography algorithms. Like in [13] an evaluation operation was performed to compare the top encryption algorithms, the authors compared these algorithms with respect to the encryption, decryption and packet size. Referring to the results shown below in figure 1, they concluded that AES is much better than RSA and DES.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| S.no | Algorithm | Packet Size (KB) | Encryption time(sec) | Decryption time(sec) |
| 1. | AES | 153 | 1.6 | 1 |
|  | DES | 153 | 3.0 | 1.1 |
|  | RSA | 153 | 7.3 | 4.9 |
| 2. | AES | 868 | 2.0 | 1.8 |
|  | DES | 868 | 4.0 | 1.2 |
|  | RSA | 868 | 8.2 | 5.1 |

**Methodology**

The execution of the proposed investigation was separated into 3 stages- encryption and encoding, steganography, and unscrambling. Within the to begin with stage, the secret word was scrambled utilizing AES-256 and encoded in Base64 i.e. different of 4, as we part the secret word into 4 pieces. In stage II we performed steganography by covering up the scrambled pieces of watchword behind the pictures by implementing another lever of AES-256 encryption. Within the last stage III, we recovered the password by unscrambling the pieces of the secret word and combining them within the redress arrangement.

Concurring to the examination worn out the writing audit, it is evident that keeping the delicate data at the decentralized area by executing a more grounded encryption calculation like AES-128 and combining it with other security strategies like steganography upraises the security of the system. Consequently, the inquiry about centers on the security of the capacity framework by bringing in the attention towards the way in which the touchy data is put away, encryption, image steganography, and secret word part strategy.

**Problem Definition**

In today's world of modernization and the web, client confirmation and security have been the foremost imperative need in many organizations and companies. There's a considerable inquiry within the field of information privacy. Unfortunately, the strategies of putting away and covering up touchy data like passwords and personal data have fizzled to fetch enough consideration from the analysts. Within the last decade, a parcel of analysts recommended the utilization of a combination of security strategies like steganography and cryptography to elevate the security of the framework. In any case, it still does not guarantee sufficient information security. In this paper, we propose a framework that executes numerous encryption strategies with a decentralized and distributed capacity of delicate data of clients and offers multi-layered security to the system. In this plan, we scramble the information utilizing AES-128, split it into pieces, and stow away it behind the pictures utilizing steganography utilizing AES-128 adding another layer of encryption and storing it

**Feasibility Study**

**System Architecture**