**IT Inventory Management System**

IMAGE AND TEXT ENCRYPTION APP FOR SECURING INTERNAL TRANSFER

## SESSION: 2019-2023; GROUP: G-7.

# GROUP MEMBERS

**SYED USAMA TANVEER 105**

**SHAMRAIZ KHAN 162**

**ABID ALI 114**

### GOVT. ISLAMIA COLLEGE, CIVIL LINES, LAHORE

### AFFILIATED WITH UNIVERSITY OF THE PUNJAB, LAHORE

#### **Abstract:**

In the form of text, audio, videos and photographs, the Internet is a commonly used tool to exchange details. The long-distance exchange of information on a wide network needs encryption to secure the information from unauthorized access. The reliability of the network plays an important role in protecting data on an insecure network. Many encryption solutions have been discovered to protect the data on the network, and recent creative encryption schemes have been in demand since e-commerce ,e-banking and multimedia technologies are viewed on a regular basis on the internet. Cryptographic coding methods have lately been used primarily to protect unauthorized access to knowledge on an insecure network. Image encryption techniques are commonly used by all cryptographic techniques to transmit photos on an insecure network.The purpose of this paper is to demonstrate the few encryption techniques that are used on an insecure network to encrypt the image. To encrypt the image, this paper proposes a new encryption technique. The suggested approach encrypts the image using AES algorithm which took text encrypt it in 128 bits to 256 bits, it makes a key of encryption using password and then convert in into binary and then made an AND function on it then perform some more operations to encrypt it using hashing.

#### Introduction:

In the present age of communication there is the need of high level data security for the prospective of data communication. In this regard there is the need of image and text data security also. The encryption of text and images has become the very important and necessary component in our daily life to accomplish our security tasks. To share the information resource among the people who look for solution must have to be connected to each other to facilitate the security process. . Encryption is a process of hiding the data, where it converts the original text and image into cipher text. Encryption uses different methods to encrypt the data into different form. But with the increase growth of multimedia application, security is an important aspect in communication and storage of image and text and encryption is the way to ensure security .Our app consists of encryption of image and text which can allows users to send data more securely and save it from hacker attacks.

**Objectives:**

Our aim is to provide the security of data. The main objective is to provide a text and image encryption mechanism which provides high security level. Less computational time and efficient way to deal with difficult and intractable data. The application must be simple, easy to use and powerful. Many factors have to be considered in order to develop the application such as processing speed of image, the strength of encryption result and ease of use to end users.

**Problem Description:**

The problem of hacking of data has become more and more common over the internet. Nowadays almost all data is transferred over the computer networks using internet and it has increased the attacks over the internet. Before transmitted data it has to be encrypted for security so that it cannot be attacked by various attackers. Cryptography is a science of protection of data by encoding it into unreadable form. It is useful way of protecting the important information by using both encryption and decryption process. The encryption and decryption process depend on the key value it is called hashing. Our app consists of encryption of image and text which can allows users to send data more securely and save it from hacker attacks.

**Scope of project:**

The scope of this project is focus on targeted user, transferred images and communication.

* The scope of the project is to limit unauthorized access and provide better security during text and image transmission.
* Ensuring that no one can access the data except the intended receiver.
* In which sender and receiver included. Sender will encrypt images that turn the images to cipher image and receiver will decrypt image to get the original images.

**Requirements:**

Module: Security Management

User can secure the images and text without any difficulty. User can send data in a secure way..

**Tools/Technology:**

* HTML
* CSS
* React Native
* Node JS
* SQLITE

**Literatural review:**

1. (Cheung, L., & Newport, C,2007) In ciphertext approach attribute-based encryption (CP-ABE), each mystery key is related with a set of properties, and each ciphertext is related with an get to structure on attributes. Decryption is empowered in case and as it were in case the user's trait set fulfills the ciphertext access structure. This gives fine-grained get to control on shared information in numerous practical settings, eg, secure database and IP multicast.
2. (Seyedzade, S. M., Mirzakuchaki, S., & Atani, R. E. 2010) A novel calculation for picture encryption ased on hash work is proposed. In our calculation, a 512-bit long outside mystery key is utilized as the input esteem . To begin with of all, the hash work is adjusted to produce a key stream which is more reasonable for picture encryption. At that point the ultimate encryption key stream is created by connecting the key stream and plaintext coming about in both key affectability and plaintext affectability. This plot can accomplish tall affectability, tall complexity, and tall security through as it were two rounds of dissemination handle. Within the to begin with circular of dissemination handle, an unique picture is divided on a level plane to an cluster which comprises of 1,024 segments of measure 8 × 8. Within the moment circular, the same operation is connected vertically to the transpose of the gotten cluster.
3. (Qais H. Alsafasfeh and Aouda A. Arfoa , 2011) Image Encryption Based on the Common Approach for Different Chaotic Systemsa modern calculation by including the Lorenz chaotic framework and the Rössler chaotic framework. From investigation through explore, they appeared the points of interest of picture encryption calculation which was tall darken level and tall speed, huge key space and high-level security.
4. (Sun, Q., Yan, W., Huang, J., & Ma, W,2012) . Picture Encryption Based on Bit-plane Deterioration. At to begin with, they deteriorated a gray picture into a few bit-plane pictures. At that point we rearranged them by a irregular scrambling calculation independently. Finally, we consolidated the mixed bit-plane pictures concurring to their unique levels on bit-planes and picked up an scrambled picture. Due to each bit-plane picture is mixed by utilizing distinctive scrambling irregular arrangements, the bits found at the same arranges in numerous bit-planes are nearly not remain on the first positions when each bit-plane being mixed independently. For each pixel, its all bits of gray level, hence, may be come from those pixels found distinctive positions. Consequently, the remade gray levels of picture are changed ineluctable. It is apparent that our strategy can do both positions trade scrambling and gray level alter scrambling at the same time.
5. (Chandel, G. S., & Patel, P,2013) On the premise of their think about the creators were able discover the issue detailing as well as investigation, which empowered them to supply future upgrade headings. Based on the over consider they given the taking after future headings which can be supportive in superior location: 1) Utilize Capable encryption strategy like DES and RSA. 2) Increment RGB randomization and security key randomization for making strides picture security. 3) Move forward the piece estimate or bit encryption standard like 128 bit and 256 bit. 4) Chaos-based ciphers ought to not be helpless to conventional differential and straight cryptanalysis assaults so the utilize of hybridization is the way better plausibility
6. (Manajaih, D. H,2014) Quicker usage of public-key cryptography and in specific of RSA are of utmost importance these days. Performing quick secluded duplication for huge integrability is of special interest since it gives the premise for performing quick measured exponentiation, which is the key operation of the RSA cryptosystem. As of now, it appears that in a radix representation, all major execution changes have been accomplished
7. (Chauhan, S., & Mishra, P. K,2014) This paper proposed a secured encryption method for advanced pictures; it is similarly appropriate for any advanced record . The bit-wise XORing and moving operation were utilized to cipher a piece of mystery bytes and after that ciphered bytes were rearranged inside N places (N is the size of mystery key). Usually the combination of substitution and transposition strategy performed utilizing energetic SBOX and TBOX. The key for the proposed cryptosystem is exceptionally huge which gives way better security against brute-force assault. Besides, key affectability investigation, factual investigation and differential assault examination demonstrate the tall worthiness of the proposed calculation.
8. (Jain, A., & Rajpal, N,2015) Proposed an picture encryption strategy utilizing DNA (Deoxyribonucleic corrosive) operations and chaotic maps. Firstly, the input picture is DNA encoded and a veil is created by utilizing 1D chaotic outline. Secondl, this cover is included with the DNA encoded picture utilizing DNA expansion. The middle result is DNA complemented with the assistance of a complement network delivered by two 1D chaotic maps. At long last, the resultant framework is permuted utilizing 2D chaotic maps followed by DNA translating to urge the cipher picture. The proposed strategy is completely invertible and it can stand up to known plain content assaults, measurable assaults and differential assaults
9. (Rifki, R., Septiarini, A., & Hatta, H. R,2018) . This investigate proposes the RC4 stream cipher strategy for security in sending SMS. In any case, RC4 has any impediment within the Key Planning Calculation (KSA) and Pseudo Arbitrary Era Calculation (PRGA) stages. In this manner, this inquire about created RC4 with a random starting state to extend the haphazardness level of the keystream. This SMS cryptography strategy connected the forms of encryption against the sent SMS taken after by decoding against the gotten SMS.
10. (Bouteghrine, B., Tanougast, C. & Sadoudi,2021) In this paper, a modern calculation for colour picture encryption has been proposed. The calculation is based on a unused 3-dimensional (3-D) discrete time chaos framework which performs the dissemination and perplexity forms. The oddity of the proposed work is the unused 3-D outline characterized by five nonlinear terms and three control parameters to guarantee way better chaotic properties. Besides, the proposed modern outline is utilized to perform 3-stage encryption calculation which accomplishes superior execution whereas protecting the conventional confusion-diffusion structure.

**METHODOLOGY**

There are many models and methods which are used according to planning and developments. We are going to use "Agile Model” for creating this project. Agile software development is an iterative and incremental software development methodology that focuses on delivering software quickly, with frequent iterations and rapid response to change. It is based on the principles of iterative development, where requirements and solutions evolve through collaboration between self-organizing, cross-functional teams. Agile methods break tasks into small increments with minimal planning, and do not directly involve long-term planning. Iterations are short time frames (time boxes) that typically last from one to four weeks. Each iteration involves a team working through a full software development cycle including:

**1. Requirements gathering**

At this stage our team members will gather and analyze the requirements for Career

Counselling system. This will include identifying the user needs, functional and non-functional

requirements, and constraints of the project.

**2. Design the requirements**

This stage include designing the interface of website, designing the database of Career

Counselling and overall architecture.

3. Construction/ iteration

At this stage, the coding of the website start. This will include writing the code, configuring

the database, and integrating the various components of the system.

**4. Testing/ Quality assurance**

Testing includes the overall system is bug free and meet the requirements mentioned above.

**5. Deployment**

At this stage the system will complete and available to the users.

**6. Feedback**

The feedback from users is collected at this stage.

The Advanced Encryption Standard (AES) is a symmetric block cipher chosen by the U.S. government to protect classified information. AES is implemented in software and hardware throughout the world to encrypt sensitive data. The AES Encryption algorithm (too known as the Rijndael algorithm) may be a symmetric square cipher algorithm with a block/chunk measure of 128 bits. It changes over these person pieces utilizing keys of 128, 192, and 256 bits.

DECRYPTION

KEY

**Methods used in AES:**

To review the overall structure of AES and to focus particularly on the four steps used in each round of AES:

1. **Byte substitution**
2. **Shift rows**
3. **Mix columns**
4. **Add round key**

**References:**

1. Cheung, L., & Newport, C. (2007, October). Provably secure ciphertext policy ABE. In *Proceedings of the 14th ACM conference on Computer and communications security* (pp. 456-465). https://dl.acm.org/doi/abs/10.1145/1315245.1315302
2. Seyedzade, S. M., Mirzakuchaki, S., & Atani, R. E. (2010, October). A novel image encryption algorithm based on hash function. In *2010 6th Iranian Conference on Machine Vision and Image Processing* (pp. 1-6). IEEE.
3. Alsafasfeh, Q. H., & Arfoa, A. A. (2011). Image encryption based on the general approach for multiple chaotic systems. *J. Signal Inf. Process.*, *2*(3), 238-244
4. Sun, Q., Yan, W., Huang, J., & Ma, W. (2012, April). Image encryption based on bit-plane decomposition and random scrambling. In *2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)* (pp. 2630-2633). IEEE.
5. Chandel, G. S., & Patel, P. (2013). A review: Image encryption with RSA and RGB randomized histograms. *International Journal of Advanced Research in Computer and Communication Engineering*, *2*(0), 11.
6. Manajaih, D. H. (2014). Modular arithmetic in RSA cryptography. *International Journal of Advanced Computer Research*, *4*(4), 973.
7. Chauhan, S., & Mishra, P. K. (2014). A neoteric fractional image encryption methods based on logistic mapping. *Int J Comput Sci Eng*, *6*(4), 79-84.
8. Jain, A., & Rajpal, N. (2015). A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps. *Multimedia Tools and Applications*, *75*(10), 5455-5472
9. Rifki, R., Septiarini, A., & Hatta, H. R. (2018). Cryptography using random Rc4 stream cipher on SMS for android-based smartphones. *International Journal of Advanced Computer Science and Applications*
10. Bouteghrine, B., Tanougast, C. & Sadoudi, S. Novel image encryption algorithm based on new 3-d chaos map. *Multimed Tools Appl* **80**, 25583–25605 (2021).