Design, Implementation And Analysis Of Image Encryption And Decryption Using AES And Blowfish Algorithms

Dr. B. Srinivas Rao
Department of CSE
Gokaraju Rangaraju Institute of Engineering and Technology
Hyderabad, Telanagana

Sai Kiran reddy Rukkammolla
Department of CSE
Gokaraju Rangaraju Institute of Engineering and Technology
Hyderabad, Telanagana

Yugender Enugala
Department of CSE
Gokaraju Rangaraju Institute of Engineering and Technology
Hyderabad, Telanagana

Jithender Kondakalla
Department of CSE
Gokaraju Rangaraju Institute of Engineering and Technology
Hyderabad, Telanagana

Prathap perumandla
Department of CSE
Gokaraju Rangaraju Institute of Engineering and Technology
Hyderabad, Telanagana

ABSTRACT

Data production for transmission using any form of multimedia, including digital images, text, music, and video, is becoming more and more intriguing. Numerous techniques, including cryptography, are employed to maintain the secrecy, integrity, and confidentiality of sensitive information as well as to prevent unauthorised access. By transforming the original data into cypher data, cryptography protects it from being decrypted or altered when it is received by the recipient. In this study, we employed Arnold Cat Mapping to use confusion schemes to jumble the pixel coordinates of the coloured images. By altering the grey values of the image pixels using the traditional techniques for encrypting and decrypting digital colour images, the shuffling mechanism and diffusion mechanism are coupled to encrypt the scrambled image. The suggested techniques used traditional encryption systems like the hill cypher method and the Vegner substitution cypher system. We discovered that the hill cypher exhibits much greater security and fast speed than other approaches from all experimental and analysis methodologies utilised on some colour images to test the suggested image encryption and decryption methods. Additionally, the cypher pictures' unpredictability was increased, hiding the natural characteristics of the original images.

INTRODUCTION

The telecommunications sector has made great strides recently in the creation of technologies that provide the end user with additional bandwidth. Utilizing a computer network, users interact with their community and share their observations, learning, and experiences.Information that is shared frequently combines different media, including text, photos, audio, and video. These media items pose numerous security risks when they are transmitted across a computer network. For instance, a company's board of directors may hold online meetings to plan future marketing strategies. A rival corporation receives this knowledge from a foe who also gives it to them. Arm force uses the control room to find the enemy's location. However, a foe intercepts the signal and changes the position.

Therefore, it is essential to safeguard the data against unwanted access. Encryption is the answer. There are many different types of encryption. The algorithm's mathematical power, encryption time, and resistance to attack all factor into the choice of encryption method. Symmetric key algorithms and asymmetric key algorithms are two categories for encryption techniques. Asymmetric and single-key symmetric-key algorithms use two separate keys, respectively. To carry out the encryption/decryption procedure, a private key and public is required. The cryptographic algorithms utilised in this work are described in this section.

LITERATURE SURVEY

User:

In this programme, users must first register and check in with a user name and password. Once logged in, users must upload an image to be encrypted, and once it has been encrypted, they will receive a secret key to their registered email address.

Encryption:

Data encryption is a computational procedure that converts plaintext/cleartext (unencrypted, readable data) into ciphertext (encrypted data), which is only available to authorized users with the correct cryptographic key. Encryption, which is an essential part of the digital revolution, simply changes readable data into another form that only individuals with the appropriate password can decode and view. Encryption is a crucial data privacy security approach that keeps sensitive information out of the hands of unauthorised users,

regardless of whether your business produces, gathers, or consumes data. A very high- level explanation of what encryption is and how it functions is given on this page.

Plain Text:

Ordinary readable text before it is converted into ciphertext in cryptography is known as plaintext, as is readable text that has been recovered from encryption. Not all data inputted into or outputted by encryption methods are plaintext.

Cypher Text:

The format of the input data that encryption algorithms work on is one of the primary categorizations approaches for widely used encryption systems. Block cyphers and stream cyphers are the two popular types.

Block cipher:

A block cipher is one that uses a block of plaintext that is handled as a whole to create a block of ciphertext that is the same size. It is an encryption technique that encrypts blocks of data with a predetermined size of n bits at a time. Each block typically has a size of 64 bits, 128 bits, or 256 bits. As an illustration, a 64-bit block cypher converts 64 bits of plaintext into 64 bits of ciphertext.

DES, Triple DES, AES, IDEA, and Blowfish are some of the commonly used encryption algorithms that fall under this group.

Stream cipher:

One bit or byte of plaintext is encrypted at a time by this encryption algorithm. The key is an endless stream of pseudorandom bits. A stream cypher implementation must have an unpredictable pseudorandom number generator and never utilise the same key twice to stay secure. Stream cyphers are created to come close to the One Time Pad, an idealised cypher. The One-Time Pad, which is designed to use a key that is completely random, may be able to achieve "absolute secrecy." It is intended to be completely resistant to brute force attacks.The issue with the one-time pad is that its key must be at least as long as the plaintext in order to generate such a cipher.

Decryption:

Decryption is the process of restoring encrypted data to its original state. Typically, encryption is done in reverse. Since decryption requires a secret key or password, it decodes the information such that only an authorized user can do so.

EXISTING SYSTEM

The text data for this project is encrypted using ASCII values or any other special characters. The encrypted data was not safely sent into the mail using the current mechanism. That data is freely accessible to the hackers. There were no restrictions on the encrypted text. This makes the information easily decryptable.
The size of each share image's pixel expansion and the recovered secret image's low contrast are two major issues with the visual cryptography scheme (VCS).

Limitations of Existing Systems:

There are the following prerequisites and restrictions for encryption: You can't encrypt files that already exist. You must copy a file that isn't encrypted yet into a new file whose encryption policy rules specify that the file has to be encrypted in order to encrypt it. Note that a file's encryption characteristics are unaffected by renaming.

There are three main types of encryption: DES, AES, and RSA. We will examine these three important encryption types that customers utilize on a daily basis, however there are many more varieties than can easily be covered here. However, we are utilizing AES and Blowfish in this project.

METHODOLOGY

BLOW FISH ALOGORITHM:

Bruce Schneier created the encryption method known as Blowfish in 1993 as a replacement for the DES Encryption Technique. Since no efficient cryptanalysis method has been discovered to yet, it is substantially faster than DES and offers a good encryption rate. One of the first safe block cyphers, it can be used anybody since it is not protected by any patents.64-bits, blockSize 32-bits to 448-bit key size varying size 18 subkeys total [P-array] There are 16 rounds.There are four replacement boxes, each with 512 entries that each 32 bits.

ADVANCED ENCRYPTION STANDARD (AES) ALGORITHM:

The Advanced Encryption Standard (AES) is a cryptographic algorithm created by the National Institute of Standards and Technology (NIST) of the United States for the encryption of electronic data. NIST chose alternative key sizes of 128, 192, or 256 bits, corresponding to 10, 12, or 14 rounds of encryption respectively, to encrypt or decrypt blocks of 128-bit plaintext into blocks of 128-bit ciphertext. It is the replacement for the DES, which came out in 1977. It operates according to a symmetric-key method.

The State array, used by AES, is a 4 by 4 column-major order matrix of 8-bit bytes that is altered at each stage of encryption. Sub Bytes, Shift Rows, Mix Columns, and Add RoundKey are four separate transformation functions that the matrix goes through in the first N-1 (N is dependent on the length of the encryption key employed) rounds. Before being placed into the rounds, the matrix is subjected to the Add RoundKey function, and the final round has only three transformation functions. Each of the N+1 round keys

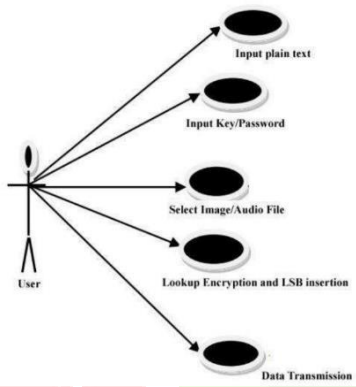
produced by the Key expansion algorithm is a unique 4 by 4 column-major order matrix.

IMPLEMENTATION

A UML Use Case Diagram is the most typical format for system requirements for software programmer. The use cases explain the desired behaviour ("What"), not the strategies for accomplishing it ("How"). Both visual and textual displays of use cases are possible. (Use case graphic, for example. One of the most crucial ideas in this modelling is the ability to create a system from the viewpoint of the end user.

By describing each visually obvious software activity, this is effective technique to explain system behavior to users in their own terms. A use case assesses the required collaboration.

Use cases are realized by assembling a society of classes and other components that work together to carry out the functionality of a use case. The society of components' static and dynamic structure is modelled.



System architecture

FUTURE WORK

In future work, we will continue on the further implementation or changes in our system and we will try to research on its further performance. However, there are still some implementation that can be applied to our system. Some of the changes that we can possibly make to the system include.
Basically, our focus is on the development of more efficient and sophisticated system for E-voting using blockchain and its related variable tools.

CONCLUSION

Using the AES technique and a 128 bit key, the image is both encrypted and decrypted. A blank form is created from the original image and key before being sent to the recipient, who will use the form to recreate the original image and key. It offers security and is a popular type inducer.

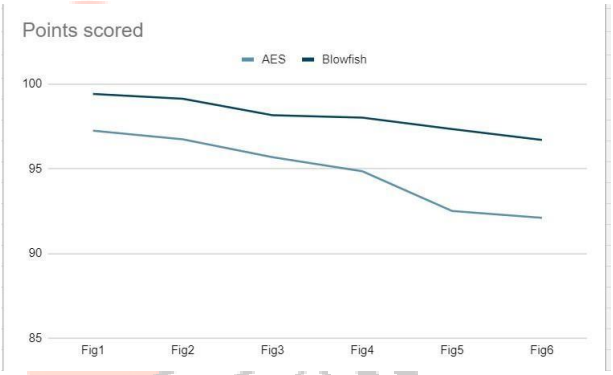
It is suggested that Blowfish, a 64 bit block cypher, replace DES. Data on 32-bit microprocessors can be encrypted using the quick algorithm blowfish. Blowfish's security has not been jeopardised. Blowfish is a symmetric block cypher with a 64-bit key that can range in length from 32 to 448 bits (14 bytes).

AES Algorithm

Image	Original Image Pixels	Decrypted Image Pixels	Percent Of Recovery
Fig.1	22,600	21,978	97.24
Fig.2	29,670	28,702	96.73
Fig.3	37,960	36,322	95.68
Fig.4	47,270	44,838	94.85
Fig.5	57,600	53,284	92.50
Fig.6	68,950	63,504	92.10

Blowfish Algorithm

Image	Original Image Pixels	Decrypted Image Pixels	Percent Of Recovery
Fig.1	22,600	22,736	99.41
Fig.2	29,670	29,412	99.13
Fig.3	37,960	37,265	98.16
Fig.4	47,270	46,332	98.01
Fig.5	57,600	56,070	97.34
Fig.6	68,950	66,736	96.70



By comparing both the algorithms we can finally conclude that blowfish algorithm is better than AES algorithm.

REFERENCES

[1] Chang-Mok Shin, Dong-Hoan Seo, Kyu-Bo Chol, Ha-Wmn Lee, and SmJmng Kim, " Multilevel Image Encryption by Binary Phase XOR Operations ", IEEE Proceeding in the year 2003.

[2] M.-R. Zhang, G.-C. Shao and K.-C. Yi, — T-matrix and its applications in image processing‖, IEEE Electronics Letters 9th December 2004 Vol. 40 No. 25

[3] Wang Ying, Zheng DeLing, Ju Lei, et al., —The Spatial-Domain Encryption of Digital Images Based on High-Dimension Chaotic System‖, Proceeding of 2004 IEEE Conference on Cybernetics and Intelligent Systems, Singapore, pp. 1172-1176, December. 2004

[4] Guosheng Gu ,Guoqiang Han "An Enhanced Chaos Based Image Encryption Algorithm", IEEE Proceedings of the First International Conference on Innovative Computing, Information and Control (ICICIC'06) in 2006.

[5] N.K. Pareek, Vinod Patidar, "Image encryption using chaotic logistic map", Elsevier, Image and Vision Computing 24 (2006) 926–934.

[6] Saroj Kumar Panigrahy, Bibhudendra Acharya and Debasish Jen, Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm 1st t International Conference on Advances in Computing, Chikhli, India, 21-22 February 2008.

[7] Mohammad Ali Bani Younes and Aman Jantan, An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption , IJCSNS International Journal of Computer Science and Network Security, VOL.8 , April 2008.

[8] Mohammad Ali Bani Younes and Aman Jantan ImageEncryption Using Block-Based Transformation Algorithm IAENG International Journal of Computer Science, 35,2008.

[9] Zhang Yun-peng, Liu Wei, Cao Shui-ping, Zhai Zheng-jun, Nie Xuan , Dai Wei-di, Digital image encryption algorithm based on chaos and improved DES, IEEE International Conference on Systems, Man and Cybernetics, 2009.

[10] Sesha Pallavi Indrakanti , P.S.Avadhani, Permutation based Image Encryption Technique, International Journal of Computer Applications (0975 – 8887) Volume 28– No.8, 2011.

[11] Amnesh Goel, Reji Mathews & Nidhi Chandra, "Image Encryption based on Inter Pixel Displacement of RGB Values inside Custom Slices", International Journal of Computer Applications (0975 – 8887), Volume 36– No.3, December 2011.

[12] Reji Mathews, Amnesh Goel, Prachur Saxena & Ved Prakash Mishra, "Image Encryption Based on Explosive Inter-pixel Displacement of the RGB Attributes of a PIXEL", Proceedings of the World Congress on Engineering and Computer Science 2011 Vol I WCECS 2011, October 19-21, 2011, San Francisco, USA. ISBN: 978-988-18210-9-6.