Gray Image and Colour Image Security using AES Algorithm

1Shaina Arora, 2Nalin Chaudhary

1Department of Computer Science and Engineering, Vivekananda Global University, Rajasthan, Jaipur
2Department of Computer Science and Engineering, Raffles University, Rajasthan, Neemrana

shaina.arora22@gmail.com

Abstract. For picture security and confirmation we utilize cryptographic. In cryptographic we scramble the information. There are various symmetric and deviated encryption procedures, which are used for encryption and unscrambling reason. Symmetric encryption approach work on ordinary key (same key utilized for encryption and unscrambling reason), but unbalanced work on with one public key and private key. Public key utilized for encryption and private key for unscrambling. The security of the stowing away is measure utilizing the MSE, PSNR, Cross-Correlation and Entropy limits. For better stowing away get the low MSE and high PSNR respects. So to make the rapid reaction we need calculation which requires some speculation and give reaction quick. From this point forward additionally take apart the time reaction of purposed assessments to additionally foster security and expedient response.

Keywords: Public Key, Private Key, Symmetric Key, Asymmetric Key, MSE, PSNR

1. Introduction

Information (text, picture, sound, video and so forth) are the most generally utilized methods of correspondence in very field typically, like the examination, industry, clinical, military and so on critical picture moves happen over an unstable web organization. Accordingly, it is important to build up sufficient security so the advanced picture or computerized picture keeps from the unapproved people to getting to discharge data. Steganography and Cryptography are the most famous strategies for information security [1]. Information assurance has come to be a weighty advanced verbal exchange downside through the web or the elective medium. Cryptography and transcription are the generally utilized procedure for information security. In cryptography information is transform one structure to another structure and in steganography restricted information is covered up into cover information [2]. Cryptography is a piece of CRYPTOLOGY where CRYPTOGRAPHY and CRYPTOANALYSIS comes. Cryptography is a technique for Protecting or Secure Information. Cryptography implies how we secure our information by utilizing ENCRYPTION and DECRYPTION calculations [3]. Cryptography can offer the going with kinds of administrations: Confidentiality (mystery); Integrity (against altering); Authentication; Non-Repudiation
2. Types of Cryptography

1. Symmetric Key Cryptography:
   It is additionally called Secret Key Cryptography or Conventional Cryptography. Symmetric Key Cryptography is an encryption system where the sender and gatherer of a message share a solitary, normal key that is used to encode and disentangle the message [4-5]. The Algorithm use is generally called a Secret key Algorithm or at times called a symmetric Algorithm. A key is a piece of information (a limit) that chooses the valuable yield of a cryptographic calculation or code.

   ![Symmetric Key Encryption](image)

   **Fig. 1 Symmetric Key Encryption**

   Symmetric Key Following Algorithms include
   - AES (Advanced Encryption Standard)
   - DES (Data Encryption Standard)
   - IDEA (International Data Encryption Algorithm)
   - Blowfish (Drop-in replacement for DES or IDEA)
   - RC4 (Rivest Cipher 4)
   - RC5 (Rivest Cipher 5)
   - RC6 (Rivest Cipher 6)

2. Asymmetric Key Cryptography:
   Asymmetric cryptography, additionally referred to call as Public-key cryptography, insinuates a cryptographic calculation which requires two separate keys, one of which is private and one of which is public. The public key is used to scramble the message and the private one is used to unscramble the message.

   Public Key Cryptography is an especially advanced kind of cryptography. Officially, it was created by Whitfield Daffier and Martin Hellman in 1975. The fundamental technique for public key cryptography was first found in 1973 by the British Clifford Cocks of Communications-Electronics Security Group (CESG) of (Government Communications Headquarters - GCHQ) but this was confidential until 1997 [6].
3. Symmetric Key Cryptography Algorithm

AES (Advance Encryption Standard):

The Advanced Encryption Standard (AES) is a symmetric square code picked by the U.S. government to ensure arranged data. AES is executed in programming and equipment all through the world to scramble delicate information. It is fundamental for government PC security, network safety and electronic information assurance.

The National Institute of Standards and Technology (NIST) began improvement of AES in 1997 when it declared the requirement for an option in contrast to the Data Encryption Standard (DES), which was beginning to become defenseless against savage power assaults.

The Advanced Encryption Standard (AES) is the solitary freely available code endorsed by the US National Security Agency (NSA) for ensuring highly confidential data. AES was first called Rijndael after its two engineers, Belgian cryptographers Vincent Rijmen and Joan Daemen.

AES Features:

NIST indicated the new AES calculation should be a square code equipped for taking care of 128-bit blocks, utilizing keys estimated at 128, 192 and 256 pieces. Different measures for being picked as the following AES calculation incorporated the accompanying:

- **Security**: Competing calculations were to be decided on their capacity to oppose assault - when contrasted with other submitted figures. Security strength was to be viewed as the main factor in the opposition.

- **Cost**: Intended to be delivered on a worldwide, nonexclusive and sovereignty free premise, the competitor calculations were to be assessed on computational and memory proficiency.
• Implementation: Factors to be considered incorporated the calculation's adaptability, reasonableness for equipment or programming execution, and generally straightforwardness.

4. Gray Scale AES Image Algorithm
   Original Image:

![Original Image](Image1)

Encrypted Image:

![Encrypted Image](Image2)

Fig 3 Gray Scale Original Image in AES Algorithm

Fig 4 Gray Scale Encrypted Image in AES Algorithm
MSE Value:

Fig 5 Gray Scale Image MSE Value in AES Algorithm

PSNR Value:

Fig 6 Gray Scale Image PSNR Value in AES Algorithm

Gray Scale AES Decrypted Image:

Fig 7 Gray Scale Decrypted Image in AES Algorithm
5. **COLOR AES ENCRYPTED IMAGE**

Original Image:

![Original Image](Image1)

Fig 8 Color Original Image in AES Algorithm

Encrypted Image:

![Encrypted Image](Image2)

Fig 9 Color Encrypted Image in AES Algorithm

MSE Value:

![MSE Value](Image3)

Fig 10 Color Image MSE Value in AES Algorithm
PSNR Value:

![PSNR Value Image]

Fig 11 Color Image PSNR Value in AES Algorithm

Decrypted Image:

![Decrypted Image]

Fig 12 Color Decrypted Image in AES Algorithm

6. AES Algorithm Gray Scale Image and Colour Image

| AES Algorithm          | MSE             | PSNR     |
|------------------------|-----------------|----------|
| AES (Gray Scale)       | 19255.0941      | 5.2853   |
| AES (Color Image)      | 20808.3643      | 4.9484   |

In Colour Image MSE three Planes Colour taken out, so it accompanies a solitary plane, so the MSE will get more from Gray Scale. PSNR conversely relative to MSE so if MSE Value Higher than PSNR Value is Low contrast with MSE.

Conversion Formula Colour to Gray Scale
0.289 R+0.5870 G+0.1140 B

7. CONCLUSION

In this Research Paper Study about Cryptography Symmetric and Asymmetric Key Cryptography and also calculated AES algorithm Gray Scale and Color Image Gray Scale difference between them. In this
we calculated MSE and PSNR value. In future we will calculate other algorithms value and also research on Steganography.

Conflict of interest
None.

References

[1] Gangadari, Bhoopal Rao, and Shaik Rafi Ahamed. "FPGA implementation of compact S-Box for AES algorithm using composite field arithmetic." 2015 Annual IEEE India Conference (INDICON). IEEE, 2015.

[2] Kalaiselvi, K., and Anand Kumar. "Enhanced AES cryptosystem by using genetic algorithm and neural network in S-box." Current Trends in Advanced Computing (ICCTAC), IEEE International Conference on. IEEE, 2016.

[3] Pammu, Ali Akbar, et al. "High Secured Low Power Multiplexer-LUT Based AES S-Box Implementation." 2016 International Conference on Information Systems Engineering (ICISE). IEEE, 2016.

[4] Liao, Nan, et al. "A high-efficient fault attack on AES S-box." Information Science and Technology (ICIST), 2016 Sixth International Conference on. IEEE, 2016.

[5] Wang, Yi, and Yajun Ha. "High throughput and resource efficient AES encryption/decryption for SANs." Circuits and Systems (ISCAS), 2016 IEEE International Symposium on. IEEE, 2016.

[6] Aryfandy Febryan, Tito Waluyo Purboyo and Randy Erfa Saputra, "Steganography Methods on Text, Audio, Image and Video: A Survey", International Journal of Applied Engineering Research, 12(21), pp-10485-10490, 2017.